

TRAITÉ DE COOPERATION EN MATIÈRE DE BREVETS

10/089662

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Commissioner
 US Department of Commerce
 United States Patent and Trademark
 Office, PCT
 2011 South Clark Place Room
 CP2/5C24
 Arlington, VA 22202
 ETATS-UNIS D'AMERIQUE
 en sa qualité d'office élu

Date d'expédition (jour/mois/année) 31 mai 2002 (31.05.02)	
Demande internationale no PCT/FR00/02717	Référence du dossier du déposant ou du mandataire 6680WO
Date du dépôt international (jour/mois/année) 29 septembre 2000 (29.09.00)	Date de priorité (jour/mois/année) 01 octobre 1999 (01.10.99)
Déposant GUILLOU, Louis etc	

1. L'office désigné est avisé de son élection qui a été faite:

☒ dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

10 avril 2001 (10.04.01)

☐ dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection ☒ a été faite

☐ n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse no de télécopieur: (41-22) 740.14.35	Fonctionnaire autorisé Christelle CROCI no de téléphone: (41-22) 338.83.38
--	--

THIS PAGE BLANK (USPTO)

TRAITE DE OPERATION EN MATIERE BREVETS

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE
en sa qualité d'office élu

Date d'expédition (jour/mois/année) 22 avril 2002 (22.04.02)	
Demande internationale no PCT/FR00/02717	Référence du dossier du déposant ou du mandataire 6680WO
Date du dépôt international (jour/mois/année) 29 septembre 2000 (29.09.00)	Date de priorité (jour/mois/année) 01 octobre 1999 (01.10.99)
Déposant GUILLOU, Louis etc	

1. L'office désigné est avisé de son élection qui a été faite:



dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

10 avril 2002 (10.04.02)



dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection



a été faite



n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse no de télécopieur: (41-22) 740.14.35	Fonctionnaire autorisé Christelle CROCI no de téléphone: (41-22) 338.83.38
--	--

THIS PAGE BLANK (USPTO)

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

10/089662

Applicant's or agent's file reference 6680WO	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/FR00/02717	International filing date (day/month/year) 29 September 2000 (29.09.00)	Priority date (day/month/year) 01 October 1999 (01.10.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant FRANCE TELECOM		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 10 April 2001 (10.04.01)	Date of completion of this report 11 March 2002 (11.03.2002)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR00/02717

I. Basis of the report

1. With regard to the elements of the international application:*

- ☐ the international application as originally filed
- ☒ the description:
pages _____ 1-67 _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☒ the claims:
pages _____ 1-18 _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☒ the drawings:
pages _____ 1/3-3/3 _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☐ the sequence listing part of the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 00/02717

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-18	YES
	Claims		NO
Inventive step (IS)	Claims	1-18	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-18	YES
	Claims		NO

2. Citations and explanations

The invention concerns a method (Claim 1) and a system (Claims 6 and 11) for proving to a controller entity the authenticity of a witness entity and/or the integrity of a message associated with said witness entity, comprising the sequence of steps consisting in commitment carried out by the witness entity, challenge carried out by the controller, response by the witness entity and checking by the controller. The invention also concerns a controller device (Claim 15) using said method.

Prior art:

EP-A-0 311 470, which is cited in the application, describes such a protocol according to which an entity called "trusted authority" assigns an identity to each entity called "witness" and calculates its RSA signature; during a personalization process, the trusted authority gives an identity and signature to the witness.

Subsequently, the witness states: "This is my identity; I know its RSA signature". The witness proves that it knows the RSA signature of its identity without disclosing it. Using the public key for RSA verification distributed by the trusted authority, an entity called "controller" verifies, without reading it, that the RSA signature

THIS PAGE BLANK (USPTO)

corresponds to the stated identity. The mechanisms using this protocol operate "without transfer of knowledge": the witness does not know the private RSA key with which the trusted authority signs a large number of identities.

Problem:

The use of the RSA technology makes the authentication process susceptible to so-called "multiplicative" attacks; moreover, the work load related to the arithmetic operations requires too much computing time for smart card applications.

Invention:

The method according to the invention does not use the RSA signature and calculates commitments R , challenges d and responses R using public/private values G_i and Q_i defined according to the features of Claim 1.

None of the documents cited in the international search report discloses or suggests the calculation steps defined in Claim 1. In particular, EP-A-0 792 044 (category X) also relates to a challenge/response authentication method, but using RSA technology.

The subject matter of Claim 1 therefore involves an inventive step (PCT Article 33).

Independent Claims 6 and 11 correspond to Claim 1 in terms of systems comprising the witness device calculating the commitments, receiving the challenges and calculating the responses. They therefore also meet the requirements of PCT Article 33.

Claims 2-5, 7-10, 12-14 and 16-18 are dependent claims and therefore likewise satisfy, as such, the PCT requirements

THIS PAGE BLANK (USPTO)

of novelty and inventive step.

Independent Claim 15 relates to a controller device using the calculation of the values G_i and Q_i of the method of the invention. Since said calculations are neither disclosed in nor suggested by the cited documents, said claim also meets the requirements of PCT Article 33.

Certain defects in the international application

In the dependent claims, the expressions "if the demonstrator has transmitted ...", "... operation ...", "if the controller ..." are used without any link to the rest of the text of the claims.

The expressions in parentheses in the claims (for example "m being greater than 1" in Claim 1) are not reference signs (PCT Rule 6.2(b)), but appear to be essential to the definition of the subject matter of the claims. The expressions should not, therefore, be in parentheses.

Certain observations on the international application

The following claims do not fully satisfy the requirement of PCT Article 6 for the following reasons:

1. Independent Claim 1:

Since the step of checking by the "controller" entity is not indicated in the claim, the wording of the subject matter of the invention ("method for proving to a controller entity the authenticity of an entity and/or the integrity of a message") is unclear, as the features disclosed in the claim relate only to the calculations of the

THIS PAGE BLANK (USPTO)

commitment/challenge/response values that can be used in the authentication method according to the invention.

Moreover, the expressions "all or part of the following parameters" and "derivatives thereof" are unclear because they may correspond to any number of combinations of the parameters defined subsequently.

2. Independent Claims 6 and 11 contain the same features as Claim 1 but expressed respectively in terms of a system and a terminal device comprising the witness device calculating commitments and responses to challenges received. The objections mentioned in paragraph 1, above, are therefore also valid for these claims.

Moreover, although Claims 6 and 11 have been drafted in the form of separate independent claims, they in fact have the same subject matter and differ from one another only by virtue of a marginal variation in the definition of the subject matter for which protection is sought (system comprising the witness or terminal device comprising the witness). Consequently, said claims considered as a whole are not concise (PCT Article 6).

3. Independent Claim 15 relates to a controller device for cooperating with the terminal or witness device. Said controller, however, does not comprise any device or system features, but does comprise method or process features, some of which, moreover, are features external to the system claimed ("unknown to the controller device"). Furthermore, said claim does not comprise challenge-producing means, which

THIS PAGE BLANK (USPTO)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 00/02717

are necessary for the authentication process described in the description as a whole. Independent Claim 15 does not therefore meet the requirement of PCT Article 6 in combination with PCT Rule 6.3(b), stipulating that an independent claim must contain all of the technical features necessary for the definition of the invention.

THIS PAGE BLANK (USPTO)

PCT

REC'D 13 MAR 2002

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL PCT

(article 36 et règle 70 du PCT)



Référence du dossier du déposant ou du mandataire 6680.WO	POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/02717	Date du dépôt international (jour/mois/année) 29/09/2000	Date de priorité (jour/mois/année) 01/10/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/32		
Déposant FRANCE TELECOM et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.
2. Ce RAPPORT comprend 7 feuilles, y compris la présente feuille de couverture.
 - ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

- I ☒ Base du rapport
- II ☐ Priorité
- III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- IV ☐ Absence d'unité de l'invention
- V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- VI ☐ Certains documents cités
- VII ☐ Irrégularités dans la demande internationale
- VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 10/04/2001	Date d'achèvement du présent rapport 11.03.2002
Nom et adresse postale de l'administration chargée de l'examen préliminaire international:  Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Cretaine, P N° de téléphone +49 89 2399 8828 

THIS PAGE BLANK (USPTO)

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/02717

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-67 version initiale

Revendications, N°:

1-18 version initiale

Dessins, feuilles:

1/3-3/3 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
- ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
- ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

THIS PAGE BLANK (USPTO)

**RAPPORT D'EXAMEN
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR00/02717

- ☐ de la description, pages :
- ☐ des revendications, n°s :
- ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui : Revendications 1-18
	Non : Revendications
Activité inventive	Oui : Revendications 1-18
	Non : Revendications
Possibilité d'application industrielle	Oui : Revendications 1-18
	Non : Revendications

- 2. Citations et explications**
voir feuille séparée

THIS PAGE BLANK (USPTO)

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

L'invention concerne un procédé (revendication 1) et un système (revendications 6 et 11) destinés à prouver à une entité contrôleur l'authenticité d'une entité témoin et/ou l'intégrité d'un message associé à cette entité témoin, comportant les étapes successives d'engagement effectuée par l'entité témoin, de défi effectué par le contrôleur, de réponse par l'entité témoin et de contrôle par le contrôleur. Elle concerne aussi un dispositif contrôleur (revendication 15) utilisant ce procédé.

Etat de la technique:

EP-A-0 311 470, cité dans la demande, décrit un tel procédé selon lequel une entité appelée "autorité de confiance" attribue une identité à chaque entité appelée "témoin" et en calcule la signature RSA; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par suite, le témoin proclame: "Voici mon identité; j'en connais la signature RSA.". Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée "contrôleur" vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant ce protocole se déroulent "sans transfert de connaissance": le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités.

Problème:

L'utilisation de la technologie RSA rend le procédé d'authentification sensible aux attaques dites "multiplicatives"; d'autre part la charge de travail liée aux opérations arithmétiques entraîne des temps de calculs trop importants pour les applications type carte à puce.

THIS PAGE BLANK (USPTO)

Invention:

Le procédé selon l'invention n'utilise pas la signature RSA et calcule des engagements R , défis d et réponses R à partir de valeurs publiques /privées G_i et Q_i définis selon les caractéristiques de la revendication 1.

Aucun des documents cités dans le rapport de recherche international ne divulgue ou suggère les étapes de calcul définies dans la revendication 1. En particulier, EP-A-0 792 044 (cat. X) se rapporte aussi à un procédé d'authentification par défi/réponse, mais utilisant la technologie RSA.

L'objet de la revendication 1 implique par conséquent une activité inventive (article 33 PCT).

Les revendications indépendantes 6 et 11 correspondent à la revendication 1 en termes de systèmes comportant le dispositif témoin calculant les engagements, recevant les défis et calculant les réponses. Elles remplissent donc aussi les conditions de l'article 33 PCT.

Les revendications 2-5, 7-10, 12-14 et 16-18 sont dépendantes et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

La revendication indépendante 15 est relative à un dispositif contrôleur utilisant les calculs de G_i et Q_i propres au procédé de l'invention. Ces calculs n'étant ni divulgués ni suggérés par les documents cités, cette revendication remplit aussi les conditions de l'article 33 PCT.

THIS PAGE BLANK (USPTO)

Irrégularités dans la demande internationale

Les expressions "cas où le démonstrateur a transmis ...", "opération de ...", "cas où le contrôleur..." dans les revendications dépendantes sont utilisées sans lien avec le reste du texte des revendications.

Les expressions entre parenthèses dans les revendications (par ex. "m étant supérieur à 1" dans la revendication 1) ne sont pas des signes de référence au sens de la Règle 6.2 b) PCT mais apparaissent essentielles à la définition de l'objet des revendications. Les expressions devraient donc apparaître sans parenthèses.

Observations relatives à la demande internationale

Les revendications suivantes ne remplissent pas entièrement les conditions de l'article 6 PCT pour les raisons suivantes:

1. revendication indépendante 1:

L'étape de contrôle par l'entité "contrôleur" n'étant pas indiquée dans la revendication, la désignation de l'objet de l'invention ("procédé destiné à prouver à une entité contrôleur l'authenticité d'une entité et/ou l'intégrité d'un message") n'est pas claire, les caractéristiques énoncées dans la revendication se rapportant uniquement aux calculs des valeurs d'engagements/défis/réponses utilisables dans le procédé d'authentification selon l'invention.

De plus les expressions "tout ou partie des paramètres suivants" et "dérivés de ceux-ci" ne sont pas claires car elles peuvent correspondre à une infinité de combinaisons des paramètres définis plus loin.

2. Les revendications indépendantes 6 et 11 contiennent les mêmes caractéristiques que la revendication 1 mais exprimées respectivement en terme de système et de dispositif terminal comportant le dispositif témoin calculant des engagements et des réponses à des défis reçus. Les objections mentionnées au paragraphe 1 ci-

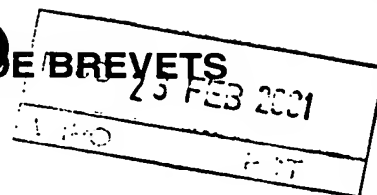
THIS PAGE BLANK (USPTO)

dessus sont donc aussi valables pour ces revendications.

De plus, bien que les revendications 6 et 11 aient été rédigées sous forme de revendications indépendantes distinctes, elles ont en fait le même objet et ne diffèrent l'une de l'autre que par une variation minimale dans la définition de l'objet pour lequel la protection est demandée (système comportant le témoin ou dispositif terminal comportant le témoin). Par conséquent ces revendications, considérées ensemble, ne sont pas concises (Article 6 PCT).

3. La revendication indépendante 15 se rapporte à un dispositif contrôleur destiné à coopérer avec le dispositif terminal ou témoin. Elle ne comporte cependant aucune caractéristique de dispositif ou système mais des caractéristiques de méthode ou procédé, dont certaines sont de plus des caractéristiques extérieures au système revendiqué ("inconnus du dispositif contrôleur"). De plus cette revendication ne comporte pas les moyens de production de défi qui sont nécessaires au processus d'authentification décrit dans la description dans son ensemble. La revendication indépendante 15 ne remplit donc pas la condition visée à l'article 6 PCT en combinaison avec la règle 6.3 b) PCT, qui prévoient qu'une revendication indépendante doit contenir toutes les caractéristiques techniques essentielles à la définition de l'invention.

THIS PAGE BLANK (USPTO)



Référence du dossier du déposant ou du mandataire BET99/118FRA	POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR99/02717	Date du dépôt international (jour/mois/année) 05/11/1999	Date de priorité (jour/mois/année) 09/11/1998
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G21C3/334		
Déposant FRAMATOME et al.		


1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.
2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

- I ☒ Base du rapport
- II ☐ Priorité
- III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- IV ☐ Absence d'unité de l'invention
- V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- VI ☐ Certains documents cités
- VII ☒ Irrégularités dans la demande internationale
- VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 08/03/2000	Date d'achèvement du présent rapport 21.02.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international:  Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Gianni, G N° de téléphone +49 89 2399 2660



THIS PAGE BLANK (USPTO)

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/02717

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17).) :

Description, pages:

1-17 version initiale

Revendications, N°:

1-16 version initiale

Dessins, feuilles:

1/11-11/11 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
- ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
- ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

THIS PAGE BLANK (USPTO)

**RAPPORT D'EXAMEN
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR99/02717

- ☐ de la description, pages :
- ☐ des revendications, n°s :
- ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui : Revendications 1,2
	Non : Revendications 3
Activité inventive	Oui : Revendications
	Non : Revendications 4-16
Possibilité d'application industrielle	Oui : Revendications 1-16
	Non : Revendications

**2. Citations et explications
voir feuille séparée**

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

THIS PAGE BLANK (USPTO)

Concernant le Point V

- 1). Le procédé de montage objet des revendications 1 et 2 n'appelle pas d'objections au titre de l'article 33 PCT.
- 2). L'objet de la revendication 3 n'est pas nouveau au titre de l'article 33(2) PCT.
- 2.1 L'expression "apte à être monté conformément au procédé selon l'une des revendications 1 ou 2", qui constitue une simple déclaration d'utilisation de l'assemblage, ne comportant aucune limitation quant à la structure de l'assemblage lui-même, n'est pas prise en compte pour l'appréciation de la nouveauté.

Le document D:GB-A-2 225 151, page 7, lignes 15-24, fig.1, 24, divulgue un assemblage de combustible pour réacteur nucléaire comportant des crayons de combustible disposés en faisceau et une ossature comprenant plusieurs ensembles de maintien 10 desdits crayons répartis sur la longueur de ces crayons, chaque ensemble comprenant une ceinture polygonale 18 possédant une configuration d'accès à son volume intérieur et une configuration de fermeture du dit volume intérieur, chaque ensemble de maintien comprenant en outre des modules de maintien 13,14,17 des crayons propres à immobiliser lesdits crayons par rapport à la ceinture et entre eux.

Un assemblage selon la revendication 1 - **sans tenir compte de l'expression "apte à ..."** ne se distingue en rien d'un assemblage divulgué par le document D.

Par conséquent, il faudrait remplacer l'expression "apte à ..." par des éléments techniques essentiels pour permettre à l'assemblage d'atteindre le but poursuivi et, **effectivement**, le rendre "apte à ..."

La demanderesse devrait tenir compte de ce que l'étendue de la protection conférée par le brevet est déterminée, non par les résultats que l'invention

THIS PAGE BLANK (USPTO)

souhaite atteindre, encore moins par les buts ou intentions poursuivis, mais plutôt par des éléments techniques essentiels pour l'invention - tels qu'ils sont inclus dans les revendications et en particulier dans les revendications indépendantes.

Ainsi donc les éléments techniques qui sont inclus dans la revendication 3 sont connus par la divulgation du document D.

L'absence de nouveauté de l'objet de la revendication 3 provient du fait que l'énoncé actuel est vague et que son étendue est beaucoup trop large et, par conséquent, peut être facilement anticipée.

- 3). Les caractéristiques divulguées dans les revendications 4 - 16 ne sont pas inventives car elles concernent des modifications qui sont une pratique courante de l'homme de l'art et les avantages qui en résultent sont aisément prévisibles.

Concernant le Point VII

- 1). La description ne cite pas de document reflétant l'état de la technique décrit à la page 1 (règle 5.1 a) ii) PCT).

THIS PAGE BLANK (USPTO)

Expéditeur: L'ADMINISTRATION CHARGÉE DE
L'EXAMEN PRÉLIMINAIRE INTERNATIONAL

14 MARS 2002

PCT

NOTIFICATION DE TRANSMISSION DU
RAPPORT D'EXAMEN PRÉLIMINAIRE
INTERNATIONAL
(règle 71.1 du PCT)

Destinataire:

VIDON, P.
CABINET PATRICE VIDON
Le Nobel
2, allée Antoine Becquerel
BP 90333
F-35703 RENNES Cédex 7
FRANCE

Date d'expédition
(jour/mois/année) 11.03.2002

Référence du dossier du déposant ou du mandataire
6680.WO

NOTIFICATION IMPORTANTE

Demande internationale No.
PCT/FR00/02717

Date du dépôt international (jour/mois/année)
29/09/2000

Date de priorité (jour/mois/année)
01/10/1999

Déposant
FRANCE TELECOM et al.

1. Il est notifié au déposant que l'administration chargée de l'examen préliminaire international a établi le rapport d'examen préliminaire international pour la demande internationale et le lui transmet ci-joint, accompagné, le cas échéant, de ces annexes.
2. Une copie du présent rapport et, le cas échéant, de ses annexes est transmise au Bureau international pour communication à tous les offices élus.
3. Si tel ou tel office élu l'exige, le Bureau international établira une traduction en langue anglaise du rapport (à l'exclusion des annexes de celui-ci) et la transmettra aux offices intéressés.

4. RAPPEL

Pour aborder la phase nationale auprès de chaque office élu, le déposant doit accomplir certains actes (dépôt de traduction et paiement des taxes nationales) dans le délai de 30 mois à compter de la date de priorité (ou plus tard pour ce qui concerne certains offices) (article 39.1) (voir aussi le rappel envoyé par le Bureau international dans le formulaire PCT/IB/301).

Lorsqu'une traduction de la demande internationale doit être remise à un office élu, elle doit comporter la traduction de toute annexe du rapport d'examen préliminaire international. Il appartient au déposant d'établir la traduction en question et de la remettre directement à chaque office élu intéressé.

Pour plus de précisions en ce qui concerne les délais applicables et les exigences des offices élus, voir le Volume II du Guide du déposant du PCT.

Nom et adresse postale de l'administration chargée de l'examen préliminaire international



Office européen des brevets
D-80298 Munich
Tél. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Fonctionnaire autorisé

Barrio Baranano, A

Tél.+49 89 2399-8621



THIS PAGE BLANK (USPTO)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire 6680.WO	POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/02717	Date du dépôt international (jour/mois/année) 29/09/2000	Date de priorité (jour/mois/année) 01/10/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/32		
Déposant FRANCE TELECOM et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.



2. Ce RAPPORT comprend 7 feuilles, y compris la présente feuille de couverture.

☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

- I ☒ Base du rapport
- II ☐ Priorité
- III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- IV ☐ Absence d'unité de l'invention
- V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- VI ☐ Certains documents cités
- VII ☐ Irrégularités dans la demande internationale
- VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 10/04/2001	Date d'achèvement du présent rapport 11.03.2002
Nom et adresse postale de l'administration chargée de l'examen préliminaire International:  Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Cretaine, P N° de téléphone +49 89 2399 8828 

THIS PAGE BLANK (USPTO)

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/02717

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-67 version initiale

Revendications, N°:

1-18 version initiale

Dessins, feuilles:

1/3-3/3 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
- ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
- ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

THIS PAGE BLANK (USPTO)

**RAPPORT D'EXAMEN
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR00/02717

- ☐ de la description, pages :
- ☐ des revendications, n°s :
- ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui : Revendications 1-18
	Non : Revendications
Activité inventive	Oui : Revendications 1-18
	Non : Revendications
Possibilité d'application industrielle	Oui : Revendications 1-18
	Non : Revendications

2. Citations et explications
voir feuille séparée

THIS PAGE BLANK (USPTO)

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

L'invention concerne un procédé (revendication 1) et un système (revendications 6 et 11) destinés à prouver à une entité contrôleur l'authenticité d'une entité témoin et/ou l'intégrité d'un message associé à cette entité témoin, comportant les étapes successives d'engagement effectuée par l'entité témoin, de défi effectué par le contrôleur, de réponse par l'entité témoin et de contrôle par le contrôleur. Elle concerne aussi un dispositif contrôleur (revendication 15) utilisant ce procédé.

Etat de la technique:

EP-A-0 311 470, cité dans la demande, décrit un tel procédé selon lequel une entité appelée "autorité de confiance" attribue une identité à chaque entité appelée "témoin" et en calcule la signature RSA; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par suite, le témoin proclame: "Voici mon identité; j'en connais la signature RSA.". Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée "contrôleur" vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant ce protocole se déroulent "sans transfert de connaissance": le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités.

Problème:

L'utilisation de la technologie RSA rend le procédé d'authentification sensible aux attaques dites "multiplicatives"; d'autre part la charge de travail liée aux opérations arithmétiques entraîne des temps de calculs trop importants pour les applications type carte à puce.

THIS PAGE BLANK (USPTO)

Invention:

Le procédé selon l'invention n'utilise pas la signature RSA et calcule des engagements R , défis d et réponses R à partir de valeurs publiques /privées G_i et Q_i définis selon les caractéristiques de la revendication 1.

Aucun des documents cités dans le rapport de recherche international ne divulgue ou suggère les étapes de calcul définies dans la revendication 1. En particulier, EP-A-0 792 044 (cat. X) se rapporte aussi à un procédé d'authentification par défi/réponse, mais utilisant la technologie RSA.

L'objet de la revendication 1 implique par conséquent une activité inventive (article 33 PCT).

Les revendications indépendantes 6 et 11 correspondent à la revendication 1 en termes de systèmes comportant le dispositif témoin calculant les engagements, recevant les défis et calculant les réponses. Elles remplissent donc aussi les conditions de l'article 33 PCT.

Les revendications 2-5, 7-10, 12-14 et 16-18 sont dépendantes et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

La revendication indépendante 15 est relative à un dispositif contrôleur utilisant les calculs de G_i et Q_i propres au procédé de l'invention. Ces calculs n'étant ni divulgués ni suggérés par les documents cités, cette revendication remplit aussi les conditions de l'article 33 PCT.

THIS PAGE BLANK (USPTO)

Irrégularités dans la demande internationale

Les expressions "cas où le démonstrateur a transmis ...", "opération de ...", "cas où le contrôleur..." dans les revendications dépendantes sont utilisées sans lien avec le reste du texte des revendications.

Les expressions entre parenthèses dans les revendications (par ex. "m étant supérieur à 1" dans la revendication 1) ne sont pas des signes de référence au sens de la Règle 6.2 b) PCT mais apparaissent essentielles à la définition de l'objet des revendications. Les expressions devraient donc apparaître sans parenthèses.

Observations relatives à la demande internationale

Les revendications suivantes ne remplissent pas entièrement les conditions de l'article 6 PCT pour les raisons suivantes:

1. revendication indépendante 1:

L'étape de contrôle par l'entité "contrôleur" n'étant pas indiquée dans la revendication, la désignation de l'objet de l'invention ("procédé destiné à prouver à une entité contrôleur l'authenticité d'une entité et/ou l'intégrité d'un message") n'est pas claire, les caractéristiques énoncées dans la revendication se rapportant uniquement aux calculs des valeurs d'engagements/défis/réponses utilisables dans le procédé d'authentification selon l'invention.

De plus les expressions "tout ou partie des paramètres suivants" et "dérivés de ceux-ci" ne sont pas claires car elles peuvent correspondre à une infinité de combinaisons des paramètres définis plus loin.

2. Les revendications indépendantes 6 et 11 contiennent les mêmes caractéristiques que la revendication 1 mais exprimées respectivement en terme de système et de dispositif terminal comportant le dispositif témoin calculant des engagements et des réponses à des défis reçus. Les objections mentionnées au paragraphe 1 ci-

THIS PAGE BLANK (USPTO)

dessus sont donc aussi valables pour ces revendications.

De plus, bien que les revendications 6 et 11 aient été rédigées sous forme de revendications indépendantes distinctes, elles ont en fait le même objet et ne diffèrent l'une de l'autre que par une variation minime dans la définition de l'objet pour lequel la protection est demandée (système comportant le témoin ou dispositif terminal comportant le témoin). Par conséquent ces revendications, considérées ensemble, ne sont pas concises (Article 6 PCT).

3. La revendication indépendante 15 se rapporte à un dispositif contrôleur destiné à coopérer avec le dispositif terminal ou témoin. Elle ne comporte cependant aucune caractéristique de dispositif ou système mais des caractéristiques de méthode ou procédé, dont certaines sont de plus des caractéristiques extérieures au système revendiqué ("inconnus du dispositif contrôleur"). De plus cette revendication ne comportent pas les moyens de production de défi qui sont nécessaires au processus d'authentification décrit dans la description dans son ensemble. La revendication indépendante 15 ne remplit donc pas la condition visée à l'article 6 PCT en combinaison avec la règle 6.3 b) PCT, qui prévoient qu'une revendication indépendante doit contenir toutes les caractéristiques techniques essentielles à la définition de l'invention.

THIS PAGE BLANK (USPTO)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur : L'ADMINISTRATION CHARGÉE DE
LA RECHERCHE INTERNATIONALE

29 DEC. 2000

PCT

Destinataire

LE NOBEL
A l'att. de VIDON, P.
2, allée Antoine Becquerel
BP 90333
35703 Rennes Cedex 7
FRANCE

NOTIFICATION DE TRANSMISSION DU
RAPPORT DE RECHERCHE INTERNATIONALE
OU DE LA DECLARATION

(règle 44.1 du PCT)

Date d'expédition
(jour/mois/année)

29/12/2000

Référence du dossier du déposant ou du mandataire

6680W0

POUR SUITE A DONNER

voir les paragraphes 1 et 4 ci-après

Demande internationale n°

PCT/FR 00/02717

Date du dépôt international

(jour/mois/année)

29/09/2000

Déposant

FRANCE TELECOM

1. ☒ Il est notifié au déposant que le rapport de recherche internationale a été établi et lui est transmis ci-joint.

Dépôt de modifications et d'une déclaration selon l'article 19 :

Le déposant peut, s'il le souhaite, modifier les revendications de la demande internationale (voir la règle 46):

Quand? Le délai dans lequel les modifications doivent être déposées est de deux mois à compter de la date de transmission du rapport de recherche internationale ; pour plus de précisions, voir cependant les notes figurant sur la feuille d'accompagnement.

Où? Directement auprès du Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse
n° de télécopieur: (41-22)740.14.35

Pour des instructions plus détaillées, voir les notes sur la feuille d'accompagnement.

2. ☐ Il est notifié au déposant qu'il ne sera pas établi de rapport de recherche internationale et la déclaration à cet effet, prévue à l'article 17.2)a), est transmise ci-joint.

3. ☐ **En ce qui concerne la réserve** pouvant être formulée, conformément à la règle 40.2, à l'égard du paiement d'une ou de plusieurs taxes additionnelles, il est notifié au déposant que

☐ la réserve ainsi que la décision y relative ont été transmises au Bureau international en même temps que la requête du déposant tendant à ce que le texte de la réserve et celui de la décision en question soient notifiés aux offices désignés.

☐ la réserve n'a encore fait l'objet d'aucune décision; dès qu'une décision aura été prise, le déposant en sera avisé.

4. **Mesure(s) consécutive(s) :** Il est rappelé au déposant ce qui suit:

Peu après l'expiration d'un délai de **18 mois** à compter de la date de priorité, la demande internationale sera publiée par le Bureau international. Si le déposant souhaite éviter ou différer la publication, il doit faire parvenir au Bureau international une déclaration de retrait de la demande internationale, ou de la revendication de priorité, conformément aux règles 90bis.1 et 90bis.3, respectivement, avant l'achèvement de la préparation technique de la publication internationale.

Dans un délai de **19 mois** à compter de la date de priorité, le déposant doit présenter la demande d'examen préliminaire international s'il souhaite que l'ouverture de la phase nationale soit reportée à 30 mois à compter de la date de priorité (ou même au-delà dans certains offices).

Dans un délai de **20 mois** à compter de la date de priorité, le déposant doit accomplir les démarches prescrites pour l'ouverture de la phase nationale auprès de tous les offices désignés qui n'ont pas été élus dans la demande d'examen préliminaire international ou dans une élection ultérieure avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou qui ne pouvaient pas être élus parce qu'ils ne sont pas liés par le chapitre II.

Nom et adresse postale de l'administration chargée de la recherche internationale



Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Hans Pettersson

THIS PAGE BLANK (USPTO)

Les présentes notes sont destinées à donner les instructions essentielles concernant le dépôt de modifications selon l'article 19. Les notes sont fondées sur les exigences du Traité de coopération en matière de brevets (PCT), du règlement d'exécution et des instructions administratives du PCT. En cas de divergence entre les présentes notes et ces exigences, ce sont ces dernières qui priment. Pour de plus amples renseignements, on peut aussi consulter le Guide du déposant du PCT, qui est une publication de l'OMPI.

Dans les présentes notes, les termes "article", "règle" et "instruction" renvoient aux dispositions du traité, de son règlement d'exécution et des instructions administratives du PCT, respectivement.

INSTRUCTIONS CONCERNANT LES MODIFICATIONS SELON L'ARTICLE 19

Après réception du rapport de recherche internationale, le déposant a la possibilité de modifier une fois les revendications de la demande internationale. On notera cependant que, comme toutes les parties de la demande internationale (revendications, description et dessins) peuvent être modifiées au cours de la procédure d'examen préliminaire international, il n'est généralement pas nécessaire de déposer de modifications des revendications selon l'article 19 sauf, par exemple, au cas où le déposant souhaite que ces dernières soient publiées aux fins d'une protection provisoire ou à une autre raison de modifier les revendications avant la publication internationale. En outre, il convient de rappeler que l'obtention d'une protection provisoire n'est possible que dans certains Etats.

Quelles parties de la demande internationale peuvent être modifiées?

Selon l'article 19, les revendications exclusivement.

Durant la phase internationale, les revendications peuvent aussi être modifiées (ou modifiées à nouveau) selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international. La description et les dessins ne peuvent être modifiées que selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international.

Lors de l'ouverture de la phase nationale, toutes les parties de la demande internationale peuvent être modifiées selon l'article 28 ou, le cas échéant, selon l'article 41.

Quand?

Dans un délai de deux mois à compter de la date de transmission du rapport de recherche internationale ou de 16 mois à compter de la date de priorité, selon l'échéance la plus tardive. Il convient cependant de noter que les modifications seront réputées avoir été reçues en temps voulu si elles parviennent au Bureau international après l'expiration du délai applicable mais avant l'achèvement de la préparation technique de la publication internationale (règle 46.1).

Où ne pas déposer les modifications?

Les modifications ne peuvent être déposées qu'auprès du Bureau international; elles ne peuvent être déposées ni auprès de l'office récepteur ni auprès de l'administration chargée de la recherche internationale (règle 46.2).

Lorsqu'une demande d'examen préliminaire international a été/est déposée, voir plus loin.

Comment?

Soit en supprimant entièrement une ou plusieurs revendications, soit en ajoutant une ou plusieurs revendications nouvelles ou encore en modifiant le texte d'une ou de plusieurs des revendications telles que déposées.

Une feuille de remplacement doit être remise pour chaque feuille des revendications qui, en raison d'une ou de plusieurs modifications, diffère de la feuille initialement déposée.

Toutes les revendications figurant sur une feuille de remplacement doivent être numérotées en chiffres arabes. Si une revendication est supprimée, il n'est pas obligatoire de renuméroter les autres revendications. Chaque fois que des revendications sont renumérotées, elles doivent l'être de façon continue (instruction 205.b)).

Les modifications doivent être effectuées dans la langue dans laquelle la demande internationale est publiée.

Quels documents doivent/peuvent accompagner les modifications?

Lettre (Instruction 205.b)):

Les modifications doivent être accompagnées d'une lettre.

La lettre ne sera pas publiée avec la demande internationale et les revendications modifiées. Elle ne doit pas être confondue avec la "déclaration selon l'article 19.1)" (voir plus loin sous "Déclaration selon l'article 19.1)").

La lettre doit être rédigée en anglais ou en français, au choix du déposant. Cependant, si la langue de la demande internationale est l'anglais, la lettre doit être rédigée en anglais; si la langue de la demande internationale est le français, la lettre doit être rédigée en français.

THIS PAGE BLANK (USPTO)

NOTES RELATIVES AU FORMULAIRE PCT/ISA/220 (suite)

La lettre doit indiquer les différences existant entre les revendications telles que déposées et les revendications telles que modifiées. Elle doit indiquer en particulier, pour chaque revendication figurant dans la demande internationale (étant entendu que des indications identiques concernant plusieurs revendications peuvent être groupées), si

- i) la revendication n'est pas modifiée;
- ii) la revendication est supprimée;
- iii) la revendication est nouvelle;
- iv) la revendication remplace une ou plusieurs revendications telles que déposées;
- v) la revendication est le résultat de la division d'une revendication telle que déposée.

Les exemples suivants illustrent la manière dont les modifications doivent être expliquées dans la lettre d'accompagnement:

1. [Lorsque le nombre des revendications déposées initialement s'élevait à 48 et qu'à la suite d'une modification de certaines revendications il s'élève à 51]:
"Revendications 1 à 15 remplacées par les revendications modifiées portant les mêmes numéros; revendications 30, 33 et 36 pas modifiées; nouvelles revendications 49 à 51 ajoutées."
2. [Lorsque le nombre des revendications déposées initialement s'élevait à 15 et qu'à la suite d'une modification de toutes les revendications il s'élève à 11]:
"Revendications 1 à 15 remplacées par les revendications modifiées 1 à 11."
3. [Lorsque le nombre des revendications déposées initialement s'élevait à 14 et que les modifications consistent à supprimer certaines revendications et à en ajouter de nouvelles]:
"Revendications 1 à 6 et 14 pas modifiées; revendications 7 à 13 supprimées; nouvelles revendications 15, 16 et 17 ajoutées." ou
"Revendications 7 à 13 supprimées; nouvelles revendications 15, 16 et 17 ajoutées; toutes les autres revendications pas modifiées."
4. [Lorsque plusieurs sortes de modifications sont faites]:
"Revendications 1-10 pas modifiées; revendications 11 à 13, 18 et 19 supprimées; revendications 14, 15 et 16 remplacées par la revendication modifiée 14; revendication 17 divisée en revendications modifiées 15, 16 et 17; nouvelles revendications 20 et 21 ajoutées."

"Déclaration selon l'article 19.1)" (Règle 46.4)

Les modifications peuvent être accompagnées d'une déclaration expliquant les modifications et précisant l'incidence que ces dernières peuvent avoir sur la description et sur les dessins (qui ne peuvent pas être modifiés selon l'article 19.1)).

La déclaration sera publiée avec la demande internationale et les revendications modifiées.

Elle doit être rédigée dans la langue dans laquelle la demande internationale est publiée.

Elle doit être succincte (ne pas dépasser 500 mots si elle est établie ou traduite en anglais).

Elle ne doit pas être confondue avec la lettre expliquant les différences existant entre les revendications telles que déposées et les revendications telles que modifiées, et ne la remplace pas. Elle doit figurer sur une feuille distincte et doit être munie d'un titre permettant de l'identifier comme telle, constitué de préférence des mots "Déclaration selon l'article 19.1)"

Elle ne doit contenir aucun commentaire dénigrant relatif au rapport de recherche internationale ou à la pertinence des citations que ce dernier contient. Elle ne peut se référer à des citations se rapportant à une revendication donnée et contenues dans le rapport de recherche internationale qu'en relation avec une modification de cette revendication.

Conséquence du fait qu'une demande d'examen préliminaire international ait déjà été présentée

Si, au moment du dépôt de modifications effectuées en vertu de l'article 19, une demande d'examen préliminaire international a déjà été présentée, le déposant doit de préférence, lors du dépôt des modifications auprès du Bureau international, déposer également une copie de ces modifications auprès de l'administration chargée de l'examen préliminaire international (voir la règle 62.2a), première phrase).

Conséquence au regard de la traduction de la demande internationale lors de l'ouverture de la phase nationale

L'attention du déposant est appelée sur le fait qu'il peut avoir à remettre aux offices désignés ou élus, lors de l'ouverture de la phase nationale, une traduction des revendications telles que modifiées en vertu de l'article 19 au lieu de la traduction des revendications telles que déposées ou en plus de celle-ci.

Pour plus de précisions sur les exigences de chaque office désigné ou élu, voir le volume II du Guide du déposant du PCT.

THIS PAGE BLANK (USPTO)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire 6680W0	POUR SUITE voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après A DONNER	
Demande internationale n° PCT/FR 00/ 02717	Date du dépôt international(jour/mois/année) 29/09/2000	(Date de priorité (la plus ancienne) (jour/mois/année) 01/10/1999
Déposant FRANCE TELECOM		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

☒ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. Base du rapport

- a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.
- ☐ la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.
- b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :
- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposée avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3. ☐ Il y a absence d'unité de l'invention (voir le cadre II).

4. En ce qui concerne le **titre**,

- ☐ le texte est approuvé tel qu'il a été remis par le déposant.
- ☒ Le texte a été établi par l'administration et a la teneur suivante:

PROCEDE, SYSTEME, DISPOSITIF A PROUVER L'AUTHEENTICITE D'UN ENTITE OU
L'INTEGRITE D'UN MESSAGE

5. En ce qui concerne l'**abrégé**,

- ☒ le texte est approuvé tel qu'il a été remis par le déposant
- ☐ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des **dessins** à publier avec l'abrégé est la Figure n°

- ☐ suggérée par le déposant.
- ☐ parce que le déposant n'a pas suggéré de figure.
- ☐ parce que cette figure caractérise mieux l'invention.

☐ Aucune des figures n'est à publier.

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 00/02717

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	EP 0 792 044 A (FUJI XEROX CO LTD) 27 August 1997 (1997-08-27) column 9, line 39 -column 12, line 38 figure 3 ----	1,6,11, 12,15 2,7,16
A	WO 96 33567 A (GEMPLUS CARD INT ;NACCACHE DAVID (FR)) 24 October 1996 (1996-10-24) page 2, line 27 -page 4, line 12 page 15, line 31 -page 18, line 17 ----	3,4,8,9, 13,14, 17,18
A	WO 89 11706 A (NCR CO) 30 November 1989 (1989-11-30) page 10, line 2 -page 11, line 6 page 12, line 21 -page 14, line 6 ----- -/--	3,4,8,9, 13,14, 17,18

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *G* document member of the same patent family

Date of the actual completion of the international search

14 December 2000

Date of mailing of the international search report

29/12/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Masche, C

INTERNATIONAL SEARCH REPORT

Internationa l Application No

PCT/FR 00/02717

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 311 470 A (TELEDIFFUSION FSE ;FRANCE ETAT (FR); PHILIPS NV (NL)) 12 April 1989 (1989-04-12) cited in the application abstract column 12, line 30 -column 13, line 55 -----	1,6,11, 15
A	QUISQUATER J -J ET AL: "FAST DECIPHERMENT ALGORITHM FOR RSA PUBLIC-KEY CRYPTOSYSTEM" ELECTRONICS LETTERS, vol. 18, no. 21, 14 October 1982 (1982-10-14), pages 905-907, XP000577331 ISSN: 0013-5194 page 906, left-hand column, line 32 - line 61 -----	1,6,11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 00/02717

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0792044 A	27-08-1997	JP 10247905 A	14-09-1998
		US 5987134 A	16-11-1999
WO 9633567 A	24-10-1996	FR 2733378 A	25-10-1996
		FR 2733379 A	25-10-1996
		EP 0766894 A	09-04-1997
		JP 10506727 T	30-06-1998
		US 5910989 A	08-06-1999
WO 8911706 A	30-11-1989	AU 622915 B	30-04-1992
		AU 3733589 A	12-12-1989
		CA 1321649 A	24-08-1993
		DE 68904540 D	04-03-1993
		DE 68904540 T	26-08-1993
		DE 374225 T	07-02-1991
		EP 0374225 A	27-06-1990
		JP 2504435 T	13-12-1990
		US 4935962 A	19-06-1990
EP 0311470 A	12-04-1989	FR 2620248 A	10-03-1989
		AT 83573 T	15-01-1993
		AU 2197188 A	23-03-1989
		CA 1295706 A	11-02-1992
		DE 3876741 A	28-01-1993
		DE 3876741 T	24-06-1993
		ES 2037260 T	16-06-1993
		FI 884082 A,B,	08-03-1989
		JP 1133092 A	25-05-1989
		KR 9608209 B	20-06-1996
		US 5218637 A	08-06-1993
		US 5140634 A	18-08-1992

THIS PAGE BLANK (USPTO)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

PCT/FR 00/02717

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X A	EP 0 792 044 A (FUJI XEROX CO LTD) 27 août 1997 (1997-08-27) colonne 9, ligne 39 -colonne 12, ligne 38 figure 3 ---	1,6,11, 12,15 2,7,16
A	WO 96 33567 A (GEMPLUS CARD INT ;NACCACHE DAVID (FR)) 24 octobre 1996 (1996-10-24) page 2, ligne 27 -page 4, ligne 12 page 15, ligne 31 -page 18, ligne 17 ---	3,4,8,9, 13,14, 17,18
A	WO 89 11706 A (NCR CO) 30 novembre 1989 (1989-11-30) page 10, ligne 2 -page 11, ligne 6 page 12, ligne 21 -page 14, ligne 6 --- -/--	3,4,8,9, 13,14, 17,18

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- *T* document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- *X* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- *Y* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- *Z* document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

14 décembre 2000

Date d'expédition du présent rapport de recherche internationale

29/12/2000

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Masche, C

RAPPORT DE RECHERCHE INTERNATIONALE

Requête internationale No

PCT/FR 00/02717

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 311 470 A (TELEDIFFUSION FSE ; FRANCE ETAT (FR); PHILIPS NV (NL)) 12 avril 1989 (1989-04-12) cité dans la demande abrégé colonne 12, ligne 30 - colonne 13, ligne 55 ----	1,6,11, 15
A	QUISQUATER J -J ET AL: "FAST DECIPHERMENT ALGORITHM FOR RSA PUBLIC-KEY CRYPTOSYSTEM" ELECTRONICS LETTERS, vol. 18, no. 21, 14 octobre 1982 (1982-10-14), pages 905-907, XP000577331 ISSN: 0013-5194 page 906, colonne de gauche, ligne 32 - ligne 61 -----	1,6,11

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No

PCT/FR 00/02717

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0792044 A	27-08-1997	JP 10247905 A	14-09-1998
		US 5987134 A	16-11-1999
WO 9633567 A	24-10-1996	FR 2733378 A	25-10-1996
		FR 2733379 A	25-10-1996
		EP 0766894 A	09-04-1997
		JP 10506727 T	30-06-1998
		US 5910989 A	08-06-1999
WO 8911706 A	30-11-1989	AU 622915 B	30-04-1992
		AU 3733589 A	12-12-1989
		CA 1321649 A	24-08-1993
		DE 68904540 D	04-03-1993
		DE 68904540 T	26-08-1993
		DE 374225 T	07-02-1991
		EP 0374225 A	27-06-1990
		JP 2504435 T	13-12-1990
		US 4935962 A	19-06-1990
EP 0311470 A	12-04-1989	FR 2620248 A	10-03-1989
		AT 83573 T	15-01-1993
		AU 2197188 A	23-03-1989
		CA 1295706 A	11-02-1992
		DE 3876741 A	28-01-1993
		DE 3876741 T	24-06-1993
		ES 2037260 T	16-06-1993
		FI 884082 A, B,	08-03-1989
		JP 1133092 A	25-05-1989
		KR 9608209 B	20-06-1996
		US 5218637 A	08-06-1993
		US 5140634 A	18-08-1992

THIS PAGE BLANK (USPTO)

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
12 avril 2001 (12.04.2001)

PCT

(10) Numéro de publication internationale
WO 01/26279 A1

(51) Classification internationale des brevets⁷: H04L 9/32

QUISQUATER, Jean-Jacques [BE/BE]: 3, avenue des
Canards, B-1640 Rhode Saint Genese (BE).

(21) Numéro de la demande internationale:

PCT/FR00/02717

(74) Mandataire: VIDON, Patrice: Le Nobel, 2, allée Antoine
Becquerel, BP 90 333, F-35703 Rennes Cedex 7 (FR).

(22) Date de dépôt international:

29 septembre 2000 (29.09.2000)

(25) Langue de dépôt:

français

(26) Langue de publication:

français

(30) Données relatives à la priorité:

99/12465	1 octobre 1999 (01.10.1999)	FR
99/12467	1 octobre 1999 (01.10.1999)	FR
99/12468	1 octobre 1999 (01.10.1999)	FR
00/09644	21 juillet 2000 (21.07.2000)	FR

(81) États désignés (*national*): AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE,
DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU,
ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS,
LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO,
NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR,
TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés (*régional*): brevet ARIPO (GH, GM, KE,
LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien
(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen
(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU,
MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM,
GA, GN, GW, ML, MR, NE, SN, TD, TG).

(71) Déposants (*pour tous les États désignés sauf US*):
FRANCE TELECOM [FR/FR]; 6, place d'Alleray,
F-75015 Paris (FR). TELEDIFFUSION DE FRANCE
[FR/FR]; 10, rue d'Oradour-sur-Glane, F-75732 Paris
Cedex 15 (FR). MATH RIZK [BE/BE]; Verte Voie, Boîte
5, B-1348 Louvain-la-Neuve (BE).

Publiée:

— Avec rapport de recherche internationale.

(72) Inventeurs; et

(75) Inventeurs/Déposants (*pour US seulement*): GUILLOU,
Louis [FR/FR]; 16, rue de l'Ise, F-35230 Bourgbarré (FR).

En ce qui concerne les codes à deux lettres et autres abrévia-
tions, se référer aux "Notes explicatives relatives aux codes et
abréviations" figurant au début de chaque numéro ordinaire de
la Gazette du PCT.

(54) Title: METHOD, SYSTEM, DEVICE FOR PROVING AUTHENTICITY OF AN ENTITY OR INTEGRITY OF A MES-
SAGE

(54) Titre: PROCEDE, SYSTEME, DISPOSITIF A PROUVER L'AUTHEENTICITE D'UNE ENTITE OU L'INTEGRITE D'UN
MESSAGE

(57) Abstract: The invention concerns a method whereby the proof is established by: $m (\geq 1)$ pairs of private Q_i and public $G_i = g_i^2$ values; a public module n formed by the product of $f (\geq 2)$ prime factors; an exponent $v = 2^k (k > 1)$, linked by the relationships of the type: $G_i \cdot Q_i^v \equiv 1 \pmod n$ or $G_i \equiv Q_i^v \pmod n$. Among the m numbers obtained by increasing Q_i or its inverse modulo n to modulo n square, $k-1$ times rank, at least one of them is different from $\pm g_i$. Among the $2m$ equations: $x^2 \equiv g_i \pmod n$, $x^2 \equiv -g_i \pmod n$, at least one of them has solutions in x in the ring of modulo n integers.

(57) Abrégé: La preuve est établie au moyen de: $m (\geq 1)$ couples de valeurs privées Q_i et publiques $G_i = g_i^2$, un module public n constitué par le produit de $f (\geq 2)$ facteurs premiers, un exposant $v = 2^k (k > 1)$, liés par des relations du type: $G_i \cdot Q_i^v \equiv 1 \pmod n$ ou $G_i \equiv Q_i^v \pmod n$. Parmi les m nombres obtenus en élevant Q_i ou son inverse modulo n au carré modulo n , $k-1$ fois de rang, au moins l'un d'entre eux est différent de $\pm g_i$. Parmi les $2m$ équations: $x^2 \equiv g_i \pmod n$; $x^2 \equiv -g_i \pmod n$, au moins l'une d'entre elles a des solutions en x dans l'anneau des entiers modulo n .

WO 01/26279 A1

THIS PAGE BLANK (USPTO)

PROCEDE, SYSTEME, DISPOSITIF A PROUVER L'AUTHENTICITE D'UNE ENTITE OU
L'INTEGRITE D'UN MESSAGE

La présente invention concerne les procédés, les systèmes ainsi que les
dispositifs destinés à prouver l'authenticité d'une entité et/ou l'intégrité
et/ou l'authenticité d'un message.

Le brevet EP 0 311 470 B1 dont les inventeurs sont Louis Guillou et Jean-
Jacques Quisquater décrit un tel procédé. On y fera ci-après référence en le
désignant par les termes : "brevet GQ" ou "procédé GQ". Par la suite on
désignera parfois par "GQ2", "invention GQ2" ou "technologie GQ2" la
présente invention.

Selon le procédé GQ, une entité appelée " autorité de confiance " attribue
une identité à chaque entité appelée " témoin " et en calcule la signature
RSA; durant un processus de personnalisation, l'autorité de confiance
donne identité et signature au témoin. Par la suite, le témoin proclame :
" Voici mon identité ; j'en connais la signature RSA. " Le témoin prouve
sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé
publique de vérification RSA distribuée par l'autorité de confiance, une
entité appelée " contrôleur " vérifie sans en prendre connaissance que la
signature RSA correspond à l'identité proclamée. Les mécanismes utilisant
le procédé GQ se déroulent " sans transfert de connaissance ". Selon le
procédé GQ, le témoin ne connaît pas la clé privée RSA avec laquelle
l'autorité de confiance signe un grand nombre d'identités.

La technologie GQ précédemment décrite fait appel à la technologie RSA.
Mais si la technologie RSA dépend bel et bien de la factorisation du module
n, cette dépendance n'est pas une équivalence, loin s'en faut, comme le
démontrent les attaques dites "multiplicatives" contre les diverses normes
de signature numérique mettant en oeuvre la technologie RSA.

L'objectif de la technologie GQ2 est double : d'une part, améliorer les

performances par rapport à la technologie RSA ; d'autre part, éviter les problèmes inhérents à la technologie RSA. La connaissance de la clé privée GQ2 est équivalente à la connaissance de la factorisation du module n. Toute attaque au niveau des triplets GQ2 se ramène à la factorisation du module n : il y a cette fois équivalence. Avec la technologie GQ2, la charge de travail est réduite, tant pour l'entité qui signe ou qui s'authentifie que pour celle qui contrôle. Grâce à un meilleur usage du problème de la factorisation, tant en sécurité qu'en performance, la technologie GQ2 évite les inconvénients présentés par la technologie RSA.

Le procédé GQ met en œuvre des calculs modulo des nombres de 512 bits ou davantage. Ces calculs concernent des nombres ayant sensiblement la même taille élevés à des puissances de l'ordre de $2^{16} + 1$. Or les infrastructures microélectroniques existantes, notamment dans le domaine des cartes bancaires, font usage de microprocesseurs auto-programmables monolithiques dépourvus de coprocesseurs arithmétiques. La charge de travail liée aux multiples opérations arithmétiques impliquées par des procédés tels que le procédé GQ, entraîne des temps de calcul qui dans certains cas s'avèrent pénalisant pour les consommateurs utilisant des cartes bancaires pour acquitter leurs achats. Il est rappelé ici, qu'en cherchant à accroître la sécurité des cartes de paiement, les autorités bancaires posent un problème particulièrement délicat à résoudre. En effet, il faut traiter deux questions apparemment contradictoires : augmenter la sécurité en utilisant des clés de plus en plus longues et distinctes pour chaque carte tout en évitant que la charge de travail n'entraîne des temps de calcul prohibitifs pour les utilisateurs. Ce problème prend un relief particulier dans la mesure où, en outre, il convient de tenir compte de l'infrastructure en place et des composants microprocesseurs existants.

La technologie GQ2 a pour objet d'apporter une solution à ce problème tout en renforçant la sécurité.

Procédé

Plus particulièrement, l'invention concerne un procédé destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées Q_1, Q_2, \dots, Q_m et publiques G_1, G_2, \dots, G_m (**m** étant supérieur ou égal à 1),

- un module public **n** constitué par le produit de **f** facteurs premiers p_1, p_2, \dots, p_f (**f** étant supérieur ou égal à 2),

Ledit module et lesdites valeurs privées et publiques sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ ou } G_i \equiv Q_i^v \pmod{n}$$

v désignant un exposant public de la forme :

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1.

Lesdites **m** valeurs publiques G_i étant les carrés g_i^2 de **m** nombres de base g_1, g_2, \dots, g_m distincts inférieurs aux **f** facteurs premiers p_1, p_2, \dots, p_f ;

lesdits **f** facteurs premiers p_1, p_2, \dots, p_f et/ou lesdits **m** nombres de base g_1, g_2, \dots, g_m étant produits de telle sorte que les conditions suivantes soient satisfaites.

Première condition :

Selon la première condition, chacune des équations :

$$x^v \equiv g_i^2 \pmod{n} \quad (1)$$

a des solutions en **x** dans l'anneau des entiers modulo **n**.

Deuxième condition :

Selon la deuxième condition, dans le cas où $G_i \equiv Q_i^v \pmod{n}$, parmi les **m** nombres q_i obtenus en élevant Q_i au carré modulo **n**, **k-1** fois de rang, l'un

d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial).

Selon la deuxième condition, dans le cas où $G_i \cdot Q_i^v \equiv 1 \pmod n$, parmi les m nombres q_i obtenus en élevant l'inverse de Q_i modulo n au carré modulo n , $k-1$ fois de rang, l'un d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial).

Il est ici précisé que selon une notation courante $\pm g_i$ représente les nombres g_i et $n-g_i$.

Troisième condition :

Selon la troisième condition, parmi les $2m$ équations :

$$x^2 \equiv g_i \pmod n \quad (2)$$

$$x^2 \equiv -g_i \pmod n \quad (3)$$

au moins l'une d'entre elles a des solutions en x dans l'anneau des entiers modulo n .

Le procédé met en œuvre selon les étapes suivantes une entité appelée témoin disposant des f facteurs premiers p_i et/ou des m nombres de base g_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public n et/ou des m valeurs privées Q_i et/ou des $f.m$ composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \pmod{p_j}$) des valeurs privées Q_i et de l'exposant public v .

Le témoin calcule des engagements R dans l'anneau des entiers modulo n .

Chaque engagement est calculé :

- soit en effectuant des opérations du type

$$R \equiv r^v \pmod n$$

où r est un aléa tel que $0 < r < n$,

- soit

- en effectuant des opérations du type

$$R_i \equiv r_i^v \pmod{p_i}$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \dots, r_f\}$,

- puis en appliquant la méthode des restes chinois.

Le témoin reçoit un ou plusieurs défis d . Chaque défi d comporte m entiers d_i ci-après appelés défis élémentaires. Le témoin calcule à partir de chaque défi d une réponse D ,

- soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d^1} \cdot Q_2^{d^2} \cdot \dots \cdot Q_m^{d^m} \bmod n$$

- soit

- en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d^1} \cdot Q_{i,2}^{d^2} \cdot \dots \cdot Q_{i,m}^{d^m} \bmod p_i$$

- puis en appliquant la méthode des restes chinois.

Ledit procédé est tel qu'il y a autant de réponses D que de défis d que d'engagements R . Chaque groupe de nombres R , d , D constitue un triplet noté $\{R, d, D\}$.

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le procédé selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur. Ladite entité démonstrateur comprend le témoin. Lesdites entités démonstrateur et contrôleur exécutent les étapes suivantes:

• étape 1 : acte d'engagement R

A chaque appel, le témoin calcule chaque engagement R en appliquant le processus spécifié ci-dessus. Le démonstrateur transmet au contrôleur tout ou partie de chaque engagement R .

• étape 2 : acte de défi d

Le contrôleur, après avoir reçu tout ou partie de chaque engagement R , produit des défis d en nombre égal au nombre d'engagements R et transmet les défis d au démonstrateur.

• étape 3 : acte de réponse D

Le témoin calcule des réponses D à partir des défis d en appliquant le processus spécifié ci-dessus.

• étape 4 : acte de contrôle

Le démonstrateur transmet chaque réponse **D** au contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque engagement R

Dans le cas où le démonstrateur a transmis une partie de chaque engagement **R**, le contrôleur, disposant des **m** valeurs publiques **G₁, G₂, ... G_m**, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou a une relation du type,

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n .$$

Le contrôleur vérifie que chaque engagement reconstruit **R'** reproduit tout ou partie de chaque engagement **R** qui lui a été transmis,

Deuxième cas : le démonstrateur a transmis l'intégralité de chaque engagement R

Dans le cas où le démonstrateur a transmis l'intégralité de chaque engagement **R**, le contrôleur, disposant des **m** valeurs publiques **G₁, G₂, ... G_m**, vérifie que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou a une relation du type,

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n .$$

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation susceptible d'être combinée avec la première, le procédé selon l'invention est destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur. Ladite entité démonstrateur comprend le témoin.

Lesdites entités démonstrateur et contrôleur exécutent les étapes suivantes:

• étape 1 : acte d'engagement R

A chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié ci-dessus.

• **étape 2 : acte de défi d**

Le démonstrateur applique une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**. Le démonstrateur transmet le jeton **T** au contrôleur. Le contrôleur, après avoir reçu un jeton **T**, produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur.

• **étape 3 : acte de réponse D**

Le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

• **étape 4 : acte de contrôle**

Le démonstrateur transmet chaque réponse **D** au contrôleur. Le contrôleur, disposant des **m** valeurs publiques **G₁, G₂, ... G_m**, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

Puis le contrôleur applique la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'** pour reconstruire le jeton **T'**. Puis le contrôleur vérifie que le jeton **T'** est identique au jeton **T** transmis.

Signature numérique d'un message et preuve de son authenticité

Dans une troisième variante de réalisation susceptible d'être combinée aux deux précédentes, le procédé selon l'invention 1 est destiné à produire la signature numérique d'un message **M** par une entité appelée entité signataire. Ladite entité signataire comprend le témoin.

Opération de signature

Ladite entité signataire exécute une opération de signature en vue d'obtenir

un message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D**.

5 Ladite entité signataire exécute l'opération de signature en mettant en oeuvre les étapes suivantes :

• **étape 1 : acte d'engagement R**

A chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié ci-dessus.

10 • **étape 2 : acte de défi d**

Le signataire applique une fonction de hachage **h** ayant comme arguments le message **M** et chaque engagement **R** pour obtenir un train binaire. Le signataire extrait de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R**.

15 • **étape 3 : acte de réponse D**

Le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

Opération de contrôle

20 Pour prouver l'authenticité du message **M**, une entité, appelée contrôleur, contrôle le message signé. Ladite entité contrôleur disposant du message signé exécute une opération de contrôle en procédant comme suit.

• **cas où le contrôleur dispose des engagements R, des défis d, des réponses D,**

25 Dans le cas où le contrôleur dispose des engagements **R**, des défis **d**, des réponses **D** le contrôleur vérifie que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

Puis le contrôleur vérifie que le message **M**, les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$d = h(\text{message}, R)$$

• **cas où le contrôleur dispose des défis d et des réponses D**

Dans le cas où le contrôleur dispose des défis **d** et des réponses **D**, le contrôleur reconstruit, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$R' \equiv G_1^{d^1} \cdot G_2^{d^2} \cdot \dots \cdot G_m^{d^m} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d^1} \cdot G_2^{d^2} \cdot \dots \cdot G_m^{d^m} \cdot \text{ mod } n$$

Puis le contrôleur vérifie que le message **M** et les défis **d** satisfont à la fonction de hachage

$$d = h(\text{message}, R')$$

• **cas où le contrôleur dispose des engagements R et des réponses D**

Dans le cas où le contrôleur dispose des engagements **R** et des réponses **D**, le contrôleur applique la fonction de hachage et reconstruit **d'**

$$d' = h(\text{message}, R)$$

Puis, contrôleur vérifie que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'^1} \cdot G_2^{d'^2} \cdot \dots \cdot G_m^{d'^m} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'^1} \cdot G_2^{d'^2} \cdot \dots \cdot G_m^{d'^m} \cdot \text{ mod } n$$

Système

La présente invention concerne également un système destiné à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- m couples de valeurs privées Q_1, Q_2, \dots, Q_m et publiques G_1, G_2, \dots, G_m (m étant supérieur ou égal à 1),

- un module public n constitué par le produit de f facteurs premiers p_1, p_2, \dots, p_f (f étant supérieur ou égal à 2),

Ledit module et lesdites valeurs privées et publiques sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ ou } G_i \equiv Q_i^v \pmod{n}$$

v désignant un exposant public de la forme :

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1.

Lesdites m valeurs publiques G_i étant les carrés g_i^2 de m nombres de base g_1, g_2, \dots, g_m distincts inférieurs aux f facteurs premiers p_1, p_2, \dots, p_f ;

lesdits f facteurs premiers p_1, p_2, \dots, p_f et/ou lesdits m nombres de base g_1, g_2, \dots, g_m étant produits de telle sorte que les conditions suivantes soient satisfaites.

Première condition :

Selon la première condition, chacune des équations :

$$x^v \equiv g_i^2 \pmod{n} \quad (1)$$

a des solutions en x dans l'anneau des entiers modulo n .

Deuxième condition :

Selon la deuxième condition, dans le cas où $G_i \equiv Q_i^v \pmod{n}$, parmi les m nombres q_i obtenus en élevant Q_i au carré modulo n , $k-1$ fois de rang, l'un d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial).

Selon la deuxième condition, dans le cas où $G_i \cdot Q_i^v \equiv 1 \pmod{n}$, parmi les m nombres q_i obtenus en élevant l'inverse de Q_i modulo n au carré modulo n , $k-1$ fois de rang, l'un d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial).

Il est ici précisé que selon une notation courante $\pm g_i$ représente les nombres g_i et $n-g_i$.

Troisième condition :

Selon la troisième condition, parmi les $2m$ équations :

$$x^2 \equiv g_i \text{ mod } n \quad (2)$$

$$x^2 \equiv -g_i \text{ mod } n \quad (3)$$

au moins l'une d'entre elles a des solutions en x dans l'anneau des entiers modulo n .

Ledit système comprend un dispositif témoin, notamment contenu dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur. Le dispositif témoin comporte une zone mémoire contenant les f facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou le module public n et/ou les m valeurs privées Q_i et/ou les $f.m$ composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \text{ mod } p_j$) des valeurs privées Q_i et l'exposant public v . Ledit dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements R du dispositif témoin.

Les moyens de calcul permettent de calculer des engagements R dans l'anneau des entiers modulo n . Chaque engagement est calculé :

- soit en effectuant des opérations du type

$$R \equiv r^v \text{ mod } n$$

où r est un aléa produit par les moyens de production d'aléas, r étant tel que $0 < r < n$,

- soit en effectuant des opérations du type

$$R_i \equiv r_i^v \text{ mod } p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \dots, r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois.

Ledit dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis **d** du dispositif témoin, pour recevoir un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers **d_i** ci-après appelés défis élémentaires ;

- des moyens de calcul, ci après désignés les moyens de calcul des réponses **D** du dispositif témoin, pour calculer à partir de chaque défi **d** une réponse **D**,

- soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \bmod n$$

- soit en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \bmod p_i,$$

puis en appliquant la méthode des restes chinois,

Ledit dispositif témoin comporte aussi des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D**. Il y a autant de réponses **D** que de défis **d** que d'engagements **R**. Chaque groupe de nombres **R**, **d**, **D** constitue un triplet noté **{R, d, D}**.

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le système selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur,

Ledit système est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade, par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit système comporte aussi un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement;

électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ; Ledit système permet d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

5 A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion.

15 • **étape 2 : acte de défi d**

Le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R**, des défis **d** en nombre égal au nombre d'engagements **R**. Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion.

20 • **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion. Les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

25 • **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse

D au contrôleur. Le dispositif contrôleur comporte aussi :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque engagement R

Dans le cas où les moyens de transmission du démonstrateur ont transmis une partie de chaque engagement **R**, les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques $G_1, G_2, \dots G_m$, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots G_m^{dm} \cdot \text{mod } n.$$

Les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçu.

Deuxième cas : le démonstrateur a transmis l'intégralité de chaque engagement R

Dans le cas où les moyens de transmission du démonstrateur ont transmis l'intégralité de chaque engagement **R**, les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des **m** valeurs publiques $G_1, G_2, \dots G_m$, vérifient que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots G_m^{dm} \cdot \text{mod } n.$$

Cas de la preuve de l'intégrité d'un message.

Dans une deuxième variante de réalisation susceptible d'être combinée avec

la première, le système selon l'invention est destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur. Ledit système est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Ledit dispositif démonstrateur peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit système comporte aussi dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement; électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur.

Ledit système exécute les étapes suivantes :

• **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion.

• **étape 2 : acte de défi d**

Le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du démonstrateur, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer au moins un jeton **T**. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif démonstrateur, pour

transmettre chaque jeton **T**, via les moyens de connexion, au dispositif contrôleur. Le dispositif contrôleur comporte aussi des moyens de production de défis pour produire, après avoir reçu le jeton **T**, des défis **d** en nombre égal au nombre d'engagements **R**. Le dispositif contrôleur
 5 comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion.

• **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque
 10 défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion. Les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

• **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse
 15 **D** au contrôleur. Le dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques **G**₁, **G**₂, ... **G**_{*m*}, pour d'une part, calculer à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit
 20 **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

puis d'autre part, calculer en appliquant la fonction de hachage **h** ayant
 25 comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'**, un jeton **T'**.

Le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton calculé **T'** au jeton **T** reçu.

Signature numérique d'un message et preuve de son authenticité

Dans une troisième variante de réalisation susceptible d'être combinée avec l'une et/ou l'autre des deux premières, le système selon l'invention est destiné à prouver la signature numérique d'un message **M**, ci-après désigné le message signé, par une entité appelée entité signataire.

Le message signé comprend :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

Opération de signature

Ledit système est tel qu'il comporte un dispositif signataire associé à l'entité signataire. Ledit dispositif signataire est interconnecté au dispositif témoin par des moyens d'interconnexion et peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit système permet d'exécuter les étapes suivantes :

• étape 1 : acte d'engagement **R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion.

• étape 2 : acte de défi **d**

Le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer un train binaire et extraire de ce train

binaire des défis **d** en nombre égal au nombre d'engagements **R**.

• **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion.

Les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

Opération de contrôle

Pour prouver l'authenticité du message **M**, une entité appelée contrôleur, contrôle le message signé.

Ledit système comporte un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif signataire.

Le dispositif signataire associé à l'entité signataire comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif signataire, pour transmettre au dispositif contrôleur, le message signé, via les moyens de connexion. Ainsi, le dispositif contrôleur dispose d'un message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

Le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

• **cas où le dispositif contrôleur dispose des engagements R, des défis d, des réponses D,**

5 Dans le cas où le dispositif contrôleur dispose des engagements R, des défis d, des réponses D, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements R, les défis d et les réponses D satisfont à des relations du type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

10 ou à des relations du type :

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message M, les défis d et les engagements R satisfont à la fonction de hachage

$$d = h(\text{message}, R)$$

15 • **cas où le dispositif contrôleur dispose des défis d et des réponses D**

Dans le cas où le dispositif contrôleur dispose des défis d et des réponses D, les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi d et de chaque réponse D, des engagements R' satisfaisant à des relations du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

20 ou à des relations du type :

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message M et les défis d satisfont à la fonction de hachage

$$d = h(\text{message}, R')$$

25 • **cas où le dispositif contrôleur dispose des engagements R et des réponses D**

Dans le cas où le dispositif contrôleur dispose des engagements R et des

réponses **D**, les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$d' = h(\text{message}, R)$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'^1} \cdot G_2^{d'^2} \cdot \dots \cdot G_m^{d'^m} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'^1} \cdot G_2^{d'^2} \cdot \dots \cdot G_m^{d'^m} \cdot \text{ mod } n$$

Dispositif Terminal

L'invention concerne aussi un dispositif terminal associé à une entité. Le dispositif terminal se présente notamment sous la forme d'un objet nomade par exemple sous la forme d'une carte bancaire à microprocesseur. Le dispositif terminal est destiné à prouver à un dispositif contrôleur :

- l'authenticité de l'entité et/ou
- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées **Q₁, Q₂, ... Q_m** et publiques **G₁, G₂, ... G_m** (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers **p₁, p₂, ... p_f** (**f** étant supérieur ou égal à 2),

Ledit module et lesdites valeurs privées et publiques sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \text{ mod } n \text{ ou } G_i \equiv Q_i^v \text{ mod } n$$

v désignant un exposant public de la forme :

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1.

Lesdites **m** valeurs publiques **G_i** étant les carrés **g_i²** de **m** nombres de base

g_1, g_2, \dots, g_m distincts inférieurs aux f facteurs premiers p_1, p_2, \dots, p_f ;
 lesdits f facteurs premiers p_1, p_2, \dots, p_f et/ou lesdits m nombres de base g_1, g_2, \dots, g_m étant produits de telle sorte que les conditions suivantes soient satisfaites.

5 **Première condition :**

Selon la première condition, chacune des équations :

$$x^v \equiv g_i^2 \pmod{n} \quad (1)$$

a des solutions en x dans l'anneau des entiers modulo n .

Deuxième condition :

10 Selon la deuxième condition, dans le cas où $G_i \equiv Q_i^v \pmod{n}$, parmi les m nombres q_i obtenus en élevant Q_i au carré modulo n , $k-1$ fois de rang, l'un d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial).

Selon la deuxième condition, dans le cas où $G_i \cdot Q_i^v \equiv 1 \pmod{n}$, parmi les m nombres q_i obtenus en élevant l'inverse de Q_i modulo n au carré modulo n ,
 15 $k-1$ fois de rang, l'un d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial).

Il est ici précisé que selon une notation courante $\pm g_i$ représente les nombres g_i et $n-g_i$.

Troisième condition :

20 Selon la troisième condition, parmi les $2m$ équations :

$$x^2 \equiv g_i \pmod{n} \quad (2)$$

$$x^2 \equiv -g_i \pmod{n} \quad (3)$$

au moins l'une d'entre elles a des solutions en x dans l'anneau des entiers modulo n .

25 Ledit dispositif terminal comprend un dispositif témoin comportant une zone mémoire contenant les f facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou le module public n et/ou les m valeurs privées Q_i et/ou les $f.m$ composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \pmod{p_j}$) des valeurs privées Q_i et l'exposant public v .

Ledit dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements **R** du dispositif témoin, pour calculer des engagements **R** dans l'anneau des entiers modulo **n**.

Chaque engagement est calculé :

- soit en effectuant des opérations du type

$$\mathbf{R} \equiv \mathbf{r}^v \bmod n$$

ou **r** est un aléa produit par les moyens de production d'aléas, **r** étant tel que $0 < \mathbf{r} < \mathbf{n}$,

- soit en effectuant des opérations du type

$$\mathbf{R}_i \equiv \mathbf{r}_i^v \bmod p_i$$

ou **r_i** est un aléa associé au nombre premier **p_i** tel que $0 < \mathbf{r}_i < \mathbf{p}_i$, chaque **r_i** appartenant à une collection d'aléas $\{\mathbf{r}_1, \mathbf{r}_2, \dots, \mathbf{r}_t\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois.

Le dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis **d** du dispositif témoin, pour recevoir un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers **d_i** ci-après appelés défis élémentaires ;

- des moyens de calcul, ci après désignés les moyens de calcul des réponses **D** du dispositif témoin, pour calculer à partir de chaque défi **d** une réponse **D**,

- soit en effectuant des opérations du type :

$$\mathbf{D} \equiv \mathbf{r} \cdot \mathbf{Q}_1^{d1} \cdot \mathbf{Q}_2^{d2} \cdot \dots \cdot \mathbf{Q}_m^{dm} \bmod n$$

- soit en effectuant des opérations du type :

$$\mathbf{D}_i \equiv \mathbf{r}_i \cdot \mathbf{Q}_{i,1}^{d1} \cdot \mathbf{Q}_{i,2}^{d2} \cdot \dots \cdot \mathbf{Q}_{i,m}^{dm} \bmod p_i$$

puis en appliquant la méthode des restes chinois.

Ledit dispositif témoin comporte aussi des moyens de transmission pour

transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D**. Il y a autant de réponses **D** que de défis **d** que d'engagements **R**. Chaque groupe de nombres **R**, **d**, **D** constituant un triplet noté **{R, d, D}**.

Cas de la preuve de l'authenticité d'une entité

5 Dans une première variante de réalisation le dispositif terminal selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur.

Ledit dispositif terminal est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est
10 interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit dispositif démonstrateur comporte aussi des moyens de connexion
15 pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant.

20 Ledit dispositif terminal permet d'exécuter les étapes suivantes :

• étape 1 : acte d'engagement R

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié
ci-dessus.

25 Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du

démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion.

• **étapes 2 et 3 : acte de défi d, acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque
5 défi **d** provenant du dispositif contrôleur via les moyens de connexion entre
le dispositif contrôleur et le dispositif démonstrateur et via les moyens
d'interconnexion entre le dispositif démonstrateur et le dispositif témoin.
Les moyens de calcul des réponses **D** du dispositif témoin, calculent les
réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

10 • **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse
D au dispositif contrôleur qui procède au contrôle.

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation susceptible d'être combinée à la
15 première, le dispositif terminal selon l'invention est destiné à prouver à une
entité appelée contrôleur l'intégrité d'un message **M** associé à une entité
appelée démonstrateur. Ledit dispositif terminal est tel qu'il comporte un
dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif
démonstrateur est interconnecté au dispositif témoin par des moyens
20 d'interconnexion. Il peut se présenter notamment sous la forme de
microcircuits logiques dans un objet nomade par exemple sous la forme
d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit
dispositif démonstrateur comporte des moyens de connexion pour le
connecter électriquement, électromagnétiquement, optiquement ou de
25 manière acoustique, notamment via un réseau de communication
informatique, au dispositif contrôleur associé à l'entité contrôleur. Ledit
dispositif contrôleur se présente notamment sous la forme d'un terminal ou
d'un serveur distant.

Ledit dispositif terminal permet d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion.

• **étapes 2 et 3 : acte de défi d, acte de réponse D**

Le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du démonstrateur, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer au moins un jeton **T**. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif démonstrateur, pour transmettre chaque jeton **T**, via les moyens de connexion, au dispositif contrôleur.

Ledit dispositif contrôleur produit, après avoir reçu le jeton **T**, des défis **d** en nombre égal au nombre d'engagements **R**.

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin. Les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

• **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

Signature numérique d'un message et preuve de son authenticité

Dans une troisième variante de réalisation susceptible d'être combinée avec

l'une ou l'autre des deux premières, le dispositif terminal selon l'invention est destiné à produire la signature numérique d'un message **M**, ci-après désigné le message signé, par une entité appelée entité signataire.

Le message signé comprend :

- 5 - le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D**.

Ledit dispositif terminal est tel qu'il comporte un dispositif signataire associé à l'entité signataire. Ledit dispositif signataire est interconnecté au
10 dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit dispositif signataire comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement,
15 optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant.

Opération de signature

20 Ledit dispositif terminal permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-
25 après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion.

- **étape 2 : acte de défi d**

Le dispositif signataire comporte des moyens de calcul, ci-après désignés

les moyens de calcul du dispositif signataire, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R**.

5 • **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion.

Les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

10 Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

Dispositif contrôleur

15 L'invention concerne aussi un dispositif contrôleur. Le dispositif contrôleur peut se présenter notamment sous la forme d'un terminal ou d'un serveur distant associé à une entité contrôleur. Le dispositif contrôleur est destiné à contrôler :

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

20 Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs publiques **G₁, G₂, ... G_m** (**m** étant supérieur ou égal à 1),

- un module public **n** constitué par le produit de **f** facteurs premiers **p₁, p₂, ... p_f** (**f** étant supérieur ou égal à 2) inconnus du dispositif contrôleur et de l'entité contrôleur associé.

25 Ledit module et lesdites valeurs privées et publiques sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \text{mod } n \text{ ou } G_i \equiv Q_i^v \text{ mod } n$$

v désignant un exposant public de la forme :

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1.

Lesdites m valeurs publiques G_i étant les carrés g_i^2 de m nombres de base

5 g_1, g_2, \dots, g_m distincts inférieurs aux f facteurs premiers p_1, p_2, \dots, p_f ;
lesdits f facteurs premiers p_1, p_2, \dots, p_f et/ou lesdits m nombres de base g_1, g_2, \dots, g_m étant produits de telle sorte que les conditions suivantes soient satisfaites.

Première condition :

10 Selon la première condition, chacune des équations :

$$x^v \equiv g_i^2 \pmod{n} \quad (1)$$

a des solutions en x dans l'anneau des entiers modulo n.

Deuxième condition :

15 Selon la deuxième condition, dans le cas où $G_i \equiv Q_i^v \pmod{n}$, parmi les m nombres q_i obtenus en élevant Q_i au carré modulo n, k-1 fois de rang, l'un d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial).

Selon la deuxième condition, dans le cas où $G_i \cdot Q_i^v \equiv 1 \pmod{n}$, parmi les m nombres q_i obtenus en élevant l'inverse de Q_i modulo n au carré modulo n, k-1 fois de rang, l'un d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial).

20 Il est ici précisé que selon une notation courante $\pm g_i$ représente les nombres g_i et $n-g_i$.

Troisième condition :

Selon la troisième condition, parmi les 2m équations :

25
$$x^2 \equiv g_i \pmod{n} \quad (2)$$

$$x^2 \equiv -g_i \pmod{n} \quad (3)$$

au moins l'une d'entre elles a des solutions en x dans l'anneau des entiers modulo n.

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le dispositif contrôleur selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur.

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associée à l'entité démonstrateur.

Ledit dispositif contrôleur permet d'exécuter les étapes suivantes :

• **étapes 1 et 2 : acte d'engagement R, acte de défi d**

Ledit dispositif contrôleur comporte aussi des moyens de réception de tout ou partie des engagements R provenant du dispositif démonstrateur, via les moyens de connexion.

Le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu tout ou partie de chaque engagement R, des défis d en nombre égal au nombre d'engagements R, chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires.

Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis d au démonstrateur, via les moyens de connexion.

• **étapes 3 et 4 : acte de réponse D, acte de contrôle**

Ledit dispositif contrôleur comporte aussi :

- des moyens de réception des réponses D provenant du dispositif démonstrateur, via les moyens de connexion

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque

engagement R

Dans le cas où les moyens de réception du dispositif contrôleur ont reçus une partie de chaque engagement **R**, les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques **G₁, G₂, ... G_m**, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots G_m^{dm} \cdot \text{mod } n ,$$

Les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçu.

Deuxième cas : le démonstrateur a transmis l'intégralité de chaque engagement R

Dans le cas où les moyens de réception du dispositif contrôleur ont reçus l'intégralité de chaque engagement **R**, les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des **m** valeurs publiques **G₁, G₂, ... G_m**, vérifient que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots G_m^{dm} \cdot \text{mod } n .$$

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation susceptible d'être combinée avec la première, le dispositif contrôleur selon l'invention est destiné à prouver l'intégrité d'un message **M** associé à une entité appelée démonstrateur.

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associée à l'entité

démonstrateur.

Ledit dispositif contrôleur permet d'exécuter les étapes suivantes :

• **étapes 1 et 2 : acte d'engagement R, acte de défi d**

Ledit dispositif contrôleur comporte aussi des moyens de réception de
 5 jetons **T** provenant du dispositif démonstrateur, via les moyens de
 connexion. Le dispositif contrôleur comporte des moyens de production de
 défis pour produire, après avoir reçu le jeton **T**, des défis **d** en nombre égal
 au nombre d'engagements **R**, chaque défi **d** comportant **m** entiers **d_i** ci-
 après appelés défis élémentaires. Le dispositif contrôleur comporte aussi
 10 des moyens de transmission, ci-après désignés les moyens de transmission
 du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens
 de connexion.

• **étapes 3 et 4 : acte de réponse D, acte de contrôle**

Ledit dispositif contrôleur comporte des moyens de réception des réponses
 15 **D** provenant du dispositif démonstrateur, via les moyens de connexion.
 Ledit dispositif contrôleur comporte aussi des moyens de calcul, ci-après
 désignés les moyens de calcul du dispositif contrôleur, disposant des **m**
 valeurs publiques **G₁, G₂, ... G_m**, pour d'une part, calculer à partir de
 chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'**
 20 satisfaisant à une relation du type :

$$R' \equiv G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot D^v \text{ mod } n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot \text{mod } n$$

puis d'autre part, calculer en appliquant une fonction de hachage **h** ayant
 25 comme arguments le message **M** et tout ou partie de chaque engagement
 reconstruit **R'**, un jeton **T'**.

Le dispositif contrôleur comporte aussi des moyens de comparaison, ci-
 après désignés les moyens de comparaison du dispositif contrôleur, pour
 comparer le jeton calculé **T'** au jeton **T** reçu.

Signature numérique d'un message et preuve de son authenticité

Dans une troisième variante de réalisation susceptible d'être combinée avec l'une et/ou l'autre des deux premières, le dispositif contrôleur selon l'invention est destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, un message signé.

Le message signé, émis par un dispositif signataire associé à une entité signataire disposant d'une fonction de hachage **h (message, R)**, comprend:

- le message **M**,
- des défis **d** et/ou des engagements **R**,
- des réponses **D** ;

Opération de contrôle

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif signataire associée à l'entité signataire. Ledit dispositif contrôleur reçoit le message signé du dispositif signataire, via les moyens de connexion.

Le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,
- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

• **cas où le dispositif contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**,**

Dans le cas où le dispositif contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d^1} \cdot G_2^{d^2} \cdot \dots \cdot G_m^{d^m} \cdot \text{mod } n$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M**, les défis **d** et les engagements **R** satisfont à la fonction de hachage :

$$d = h(\text{message}, R)$$

• **cas où le dispositif contrôleur dispose des défis d et des réponses D**

Dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D**, les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$R' \equiv G_1^{d^1} \cdot G_2^{d^2} \cdot \dots \cdot G_m^{d^m} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d^1} \cdot G_2^{d^2} \cdot \dots \cdot G_m^{d^m} \cdot \text{mod } n$$

puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M** et les défis **d** satisfont à la fonction de hachage

$$d = h(\text{message}, R')$$

• **cas où le dispositif contrôleur dispose des engagements R et des réponses D**

Dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D**, les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$d' = h(\text{message}, R)$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'^1} \cdot G_2^{d'^2} \cdot \dots \cdot G_m^{d'^m} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'^1} \cdot G_2^{d'^2} \cdot \dots \cdot G_m^{d'^m} \cdot \text{mod } n$$

Description

Les objectifs des schémas GQ sont l'authentification dynamique d'entités et de messages ainsi que la signature numérique de messages. Ce sont des schémas « sans transfert de connaissance ». Une entité prouve : elle connaît
5 un ou plusieurs nombres privés. Une autre entité contrôle : elle connaît le ou les nombres publics correspondants. L'entité qui prouve veut convaincre l'entité qui contrôle sans révéler le ou les nombres privés, de façon à pouvoir les utiliser autant de fois que de besoin.

Chaque schéma GQ repose sur un module public composé de grands
10 nombres premiers secrets. Un exposant public v et un module public n forment ensemble une clé de vérification $\langle v, n \rangle$ signifiant « élever à la puissance v modulo n » et mise en œuvre au moyen d'une ou plusieurs équations génériques, toutes du même type, direct : $G \equiv Q^v \pmod{n}$ ou inverse : $G \times Q^v \equiv 1 \pmod{n}$. Le type a un effet sur le déroulement des
15 calculs au sein de l'entité qui contrôle, pas au sein de l'entité qui prouve ; en fait, les analyses de sécurité confondent les deux types. Chaque équation générique lie un nombre public G et un nombre privé Q formant ensemble un couple de nombres $\{G, Q\}$. En résumé, chaque schéma GQ met en œuvre un ou plusieurs couples de nombres $\{G, Q\}$ pour la même clé $\langle v, n \rangle$.

20 Une version classique de schémas GQ, appelée ici GQ1, fait appel à un schéma RSA de signature numérique. La clé de vérification $\langle v, n \rangle$ est alors une clé publique RSA où l'exposant v impair est de préférence un nombre premier. Chaque schéma GQ1 utilise en général un seul couple de nombres $\{G, Q\}$: le nombre public G est déduit de données d'identification selon un mécanisme de format qui fait partie intégrante du schéma RSA de signature
25 numérique. Le nombre privé Q ou bien son inverse modulo n est une signature RSA des données d'identification. L'entité qui prouve démontre la connaissance d'une signature RSA de ses propres données d'identification et cette preuve ne révèle pas la signature qui reste donc secrète pour être

utilisée autant de fois que de besoin.

Les schémas GQ1 mettent généralement en œuvre deux niveaux de clés : la clé privée de signature RSA est réservée à une autorité accréditant des entités se distinguant les unes des autres par des données d'identification.

5 On dit qu'un tel schéma est « basé sur l'identité ». Ainsi, un émetteur de cartes à puce utilise sa clé privée RSA à l'émission de chaque carte pour calculer un nombre privé Q qu'il inscrit comme clé privée diversifiée dans la carte ; ou encore, un client sur un réseau d'ordinateurs utilise sa clé privée RSA à chaque entrée en session pour calculer un nombre privé Q qui sera la
10 clé privée éphémère du client durant la session. Les entités qui prouvent, cartes à puce ou clients en session, connaissent une signature RSA de leurs données d'identification; elles ne connaissent pas la clé privée RSA qui, dans la hiérarchie des clés, se trouve au niveau immédiatement supérieur. Cependant, une authentification dynamique d'entités par GQ1 avec un
15 module de 768 bits au niveau d'une autorité demande à peu près la même charge de travail qu'une authentification dynamique d'entités par RSA avec un module de 512 bits à trois facteurs premiers au niveau de chaque entité, ce qui permet à l'entité qui prouve d'utiliser la technique des restes chinois en calculant un résultat modulo chacun des facteurs premiers avant de
20 calculer un résultat modulo leur produit.

Toutefois, la hiérarchie de clés entre une autorité et les entités accréditées n'est pas obligatoire. On peut utiliser GQ1 avec un module propre à l'entité qui prouve, ce qui permet d'utiliser la technique des restes chinois pour réduire les charges de travail de l'entité qui prouve, ce qui ne change pas
25 fondamentalement la charge de travail de l'entité qui contrôle, mis à part le fait qu'un module au niveau de l'entité qui prouve peut être plus court qu'un module au niveau de l'autorité, par exemple 512 bits comparés à 768 bits.

Lorsque l'entité connaît les facteurs premiers de son propre module, pourquoi faire appel à un schéma RSA de signature numérique ??

Une autre version de schémas GQ, appelée ici GQ2 élémentaire, fait appel directement au problème de la factorisation d'un module n . Dans ce contexte, « directement » signifie « sans faire appel à la signature RSA ». L'objectif de GQ2 est bien de réduire les charges de travail, non seulement de l'entité qui prouve mais aussi de l'entité qui contrôle. L'entité qui prouve démontre la connaissance d'une décomposition de son propre module et cette preuve ne révèle pas la décomposition qui reste donc secrète pour être utilisée autant de fois que de besoin. La sécurité du protocole GQ2 est équivalente à la factorisation du module.

Chaque entité qui prouve dispose de son propre module n . Chaque schéma GQ2 met en œuvre un paramètre k , petit nombre plus grand que 1 fixant un exposant public $v = 2^k$, et un ou plusieurs couples de nombres $\{G_1, Q_1\}$ à $\{G_m, Q_m\}$. Chaque nombre public G_i est le carré d'un petit nombre g_i plus grand que 1 et appelé « nombre de base ». Toutes les entités qui prouvent peuvent utiliser le ou les mêmes nombres publics G_1 à G_m . La factorisation du module n et le ou les nombres privés Q_1 à Q_m sont alors au même niveau dans la hiérarchie des clés. Chaque jeu de clés GQ2 élémentaires est défini par deux conditions nécessaires et suffisantes.

- Pour chaque nombre de base, aucune des deux équations $x^2 \equiv \pm g_i \pmod{n}$ n'a de solution en x dans l'anneau des entiers modulo n , c'est-à-dire que les nombres $\pm g_i$ sont deux résidus non quadratiques modulo n .

- Pour chaque nombre de base, l'équation $x^v \equiv g_i^2 \pmod{n}$ où $v = 2^k$ a des solutions en x dans l'anneau des entiers modulo n . Le nombre privé Q_i ou son inverse modulo n est n'importe laquelle de ces solutions.

Compte tenu de la deuxième condition, pour que les nombres $\pm g_i$ soient deux résidus non quadratiques modulo n , le module n doit comporter au moins deux facteurs premiers congrus à 3 (mod 4) par rapport auxquels le symbole de Legendre de g_i diffère. Par conséquent, tout module composé de facteurs premiers dont aucun ou un seul est congru à 3 (mod 4) ne permet

pas d'établir un jeu de clés GQ2 élémentaires, ce qui privilégie les facteurs premiers congrus à 3 (mod 4). Or en prenant au hasard des grands nombres premiers, il s'avère qu'ils sont environ pour moitié congrus à 3 (mod 4) et pour moitié à 1 (mod 4). De ce fait, beaucoup de modules RSA en usage ne permettent pas d'établir des jeux de clés GQ2 élémentaires.

Nous introduisons ici les jeux de clés GQ2 généralisées pour surmonter cette limitation afin de pouvoir utiliser des techniques GQ2 avec n'importe quel module, en particulier, n'importe quel module RSA ; ils reposent sur deux principes nécessaires et suffisants.

Le premier principe reproduit la deuxième condition de GQ2 élémentaire.

— Pour chaque nombre de base g_i à g_m , l'équation $x^v \equiv g_i^2 \pmod{n}$ où $v = 2^k$ a des solutions en x dans l'anneau des entiers modulo n .

Parce que le nombre privé Q_i ou bien son inverse modulo n est une solution à l'équation, $k-1$ carrés successifs modulo n le transforment en un nombre q_i qui est une racine carrée de G_i dans l'anneau des entiers modulo n . Selon que le nombre q_i est égal à l'un des deux nombres g_i ou $n-g_i$, ou différent des deux nombres g_i et $n-g_i$, nous disons qu'il est trivial ou non. Lorsqu'un nombre q_i est non trivial, n qui divise $q_i^2 - g_i^2$ ne divise ni $q_i - g_i$ ni $q_i + g_i$. Tout nombre q_i non trivial révèle donc une décomposition du module n .

$$n = \text{pgcd}(n, q_i - g_i) \times \text{pgcd}(n, q_i + g_i)$$

Le deuxième principe élargit la première condition de GQ2 élémentaire.

— Parmi les nombres q_i à q_m , au moins un nombre q_i est non trivial.

Observons que si un nombre q_i existe alors que les nombres $\pm g_i$ sont deux résidus non quadratiques dans l'anneau des entiers modulo n , le nombre q_i est manifestement non trivial. Ainsi, les jeux de clés GQ2 élémentaires font bien partie des jeux de clés GQ2 généralisées qui permettent d'utiliser n'importe quel module, c'est-à-dire toute composition de grands nombres premiers congrus indifféremment à 3 ou à 1 (mod 4) dont au moins deux sont distincts. Par contre, beaucoup de jeux de clés GQ2 généralisées ne

sont pas des jeux de clés GQ2 élémentaires. Chaque jeu de clés GQ2 généralisées est dans l'un des deux cas suivants.

- Lorsque les $2 \times m$ nombres $\pm g_1$ à $\pm g_m$ sont tous des résidus non quadratiques, c'est un jeu de clés GQ2 élémentaires.
- Lorsque parmi les $2 \times m$ nombres $\pm g_1$ à $\pm g_m$, il y a au moins un résidu quadratique, ce n'est pas un jeu de clés GQ2 élémentaires; c'est ce que nous appelons ici un jeu de clés GQ2 complémentaires.

La présente invention porte sur les jeux de clés GQ2 complémentaires, par définition, ces jeux de clés GQ2 généralisées qui ne sont pas élémentaires. Outre les deux principes précédents, un tel jeu doit satisfaire un troisième principe.

— Parmi les $2 \times m$ nombres $\pm g_1$ à $\pm g_m$, il y a au moins un résidu quadratique. Pour appréhender le problème et comprendre la solution que nous en donnons, c'est-à-dire l'invention, analysons d'abord la décomposition du module n révélée par un nombre q non trivial, puis rappelons la technique des restes chinois, puis, la notion de rang dans un corps de Galois $CG(p)$; puis, étudions les fonctions « élever au carré » dans $CG(p)$ et « prendre une racine carrée » d'un résidu quadratique dans $CG(p)$; enfin, analysons l'applicabilité des trois principes énoncés ci-dessus.

Analyse des décompositions du module — De même que le module n se décompose en f facteurs premiers p_1 à p_f , l'anneau des entiers modulo n se décompose en f corps de Galois $CG(p_1)$ à $CG(p_f)$. Dans chaque corps, il y a deux racines carrées de l'unité, à savoir ± 1 . Dans l'anneau, il y a donc 2^f racines carrées de l'unité. Chaque nombre privé q_1 à q_m définit un nombre $\Delta_i = q_i / g_i \pmod{n}$ qui est une de ces 2^f racines carrées de l'unité dans l'anneau; en d'autres termes, n divise $\Delta_i^2 - 1$.

- Lorsque q_i est trivial, c'est-à-dire $\Delta_i = \pm 1$, n divise $\Delta_i - 1$ ou bien $\Delta_i + 1$ et donc Δ_i ne révèle pas de décomposition du module n .
- Lorsque q_i est non trivial, c'est-à-dire $\Delta_i \neq \pm 1$, n ne divise ni $\Delta_i - 1$ ni $\Delta_i + 1$

et donc Δ_i révèle une décomposition, $n = \text{pgcd}(n, \Delta_i - 1) \times \text{pgcd}(n, \Delta_i + 1)$, résultant de la valeur de Δ_i dans chaque corps : le ou les facteurs premiers divisant $\Delta_i - 1$ d'un côté, celui ou ceux divisant $\Delta_i + 1$ de l'autre.

Examinons les règles de composition multiplicative des nombres q . Deux
5 nombres $\{q_1, q_2\}$ donnent un nombre composé $q_1 \times q_2 \pmod{n}$.

- Lorsque q_1 est non trivial et q_2 trivial, le nombre composé $q_1 \times q_2 \pmod{n}$ est non trivial ; il révèle la même décomposition que q_1 .

- Lorsque q_1 et q_2 sont non triviaux et $\Delta_1 = \pm \Delta_2$, le nombre composé $q_1 \times q_2 \pmod{n}$ est trivial ; il ne révèle pas de décomposition.

10 - Lorsque q_1 et q_2 sont non triviaux et $\Delta_1 \neq \pm \Delta_2$, le nombre composé $q_1 \times q_2 \pmod{n}$ est non trivial ; il révèle une troisième décomposition.

Trois nombres $\{q_1, q_2, q_3\}$ donnent quatre nombres composés $\{q_1 \times q_2, q_1 \times q_3, q_2 \times q_3, q_1 \times q_2 \times q_3 \pmod{n}\}$, soit un total de sept nombres ; m nombres donnent ainsi $2^m - m - 1$ nombres composés, soit un total de $2^m - 1$ nombres.

15 Considérons un jeu de clés GQ2 généralisées comportant i nombres de base g_1 à g_i et i nombres privés Q_1 à Q_i donnant i nombres q_1 à q_i et donc i nombres Δ_1 à Δ_i qui sont des racines de l'unité. Cherchons à prendre en compte un autre nombre de base g_{i+1} par un nombre privé Q_{i+1} donnant un nombre q_{i+1} et donc une racine Δ_{i+1} .

20 • Le total des $2^{i+1} - 1$ nombres comporte autant de nombres non triviaux dans chacun des deux cas suivants.

- La racine Δ_{i+1} est triviale et au moins une racine Δ_1 à Δ_i est non triviale.

- La racine Δ_{i+1} est non triviale et figure parmi les $2 \times i$ racines $\pm \Delta_1$ à $\pm \Delta_i$.

25 • Dans le cas où la racine Δ_{i+1} est non triviale et ne figure pas parmi les $2 \times i$ racines $\pm \Delta_1$ à $\pm \Delta_i$, chaque nombre composé où figure q_{i+1} est non trivial.

Par conséquent, lorsque parmi m nombres q_1 à q_m , au moins un est non trivial, plus de la moitié du total des $2^m - 1$ nombres sont non triviaux.

Par définition, nous disons que $l < f$ nombres non triviaux $\{q_1, q_2, \dots, q_l\}$ sont indépendants par rapport au module n lorsque chacun des $2^l - l - 1$

nombre composés correspondants est non trivial, c'est-à-dire que, au total, les 2^f-1 nombres sont tous non triviaux. Chacun de ces 2^f-1 nombres révèle alors une décomposition différente du module n .

- Lorsque les f facteurs premiers sont distincts, il y a 2^f-1 décompositions du module n . Alors, si $f-1$ nombres q sont indépendants, il y a une correspondance biunivoque entre les 2^f-1 décompositions et un total de 2^f-1 nombres comprenant les $f-1$ nombres indépendants et les 2^f-f nombres composés correspondants.

Restes chinois — Soient deux nombres a et b premiers entre eux tels que $0 < a < b$, et deux nombres X_a de 0 à $a-1$ et X_b de 0 à $b-1$; il s'agit de déterminer le nombre unique X de 0 à $a \times b - 1$ tel que $X_a \equiv X \pmod{a}$ et $X_b \equiv X \pmod{b}$. Le nombre $\alpha \equiv \{b \pmod{a}\}^{-1} \pmod{a}$ est le paramètre des restes chinois. Voici l'opération élémentaire des restes chinois.

$$x \equiv X_b \pmod{a}$$

$$y = X_a - x ; \text{ si } y \text{ est négatif, remplacer } y \text{ par } y+a$$

$$z \equiv \alpha \times y \pmod{a}$$

$$X = z \times b + X_b$$

En résumé, nous écrivons : $X = \text{Restes Chinois}(X_a, X_b)$.

Lorsque f facteurs premiers sont rangés dans l'ordre croissant, du plus petit p_1 au plus grand p_f , les paramètres des restes chinois peuvent être les suivants (il y en a un de moins que de facteurs premiers, c'est-à-dire $f-1$).

- Le premier paramètre est $\alpha \equiv (p_2 \pmod{p_1})^{-1} \pmod{p_1}$.

- Le second paramètre est $\beta \equiv (p_1 \times p_2 \pmod{p_3})^{-1} \pmod{p_3}$.

- Le i -ième paramètre est $\lambda \equiv (p_1 \times \dots \times p_{i-1} \pmod{p_i})^{-1} \pmod{p_i}$.

- Et ainsi de suite.

En $f-1$ opérations élémentaires, on établit un nombre X de 0 à $n-1$ à partir de tout jeu de f composantes de X_1 à X_f avec X_j de 0 à p_j-1 :

- un premier résultat $\pmod{p_1 \times p_2}$ avec le premier paramètre,

- puis, un second résultat $\pmod{p_1 \times p_2 \times p_3}$ avec le second paramètre,

- jusqu'au résultat final (mod $n = p_1 \times p_2 \times \dots \times p_f$) avec le dernier paramètre.

En résumé, étant donnés les facteurs premiers p_1 à p_f , chaque élément de l'anneau des entiers modulo n a deux représentations équivalentes :

- f nombres X_1 à X_f , une composante par facteur premier : $X_j \equiv X \pmod{p_j}$,

5 - un nombre X de 0 à $n-1$, $X = \text{Restes Chinois } (X_1, X_2, \dots, X_f)$.

Rang des nombres dans $\text{CG}(p)$ — Soit un nombre premier impair p et un

nombre a plus petit que p , c'est-à-dire $0 < a < p$. Par définition, le rang de a

par rapport à p est la période de la suite $\{X\}$ définie par $\{x_1 = a$; puis, pour

$i \geq 1$, $x_{i+1} \equiv a \times x_i \pmod{p}\}$. Grâce au théorème de Fermat, nous obtenons :

10 $x_{i+p} \equiv a^p \times x_i \equiv a \times x_i \equiv x_{i+1} \pmod{p}$. Par conséquent, le rang d'un nombre a par

rapport à un nombre premier p est $p-1$ ou un diviseur de $p-1$.

Par exemple, lorsque $(p-1)/2$ est un nombre premier impair p' , le corps de

Galois $\text{CG}(p)$ comporte un nombre de rang 1 : c'est 1, un nombre de rang

2 : c'est -1 , $p'-1$ nombres de rang p' et $p'-1$ nombres de rang $2 \times p' = p-1$.

15 Dans $\text{CG}(p)$, tout nombre de rang $p-1$ est un « générateur ». La dénomi-

nation est due au fait que les puissances successives d'un générateur dans

$\text{CG}(p)$, c'est-à-dire les termes de la suite $\{X\}$ pour les indices de 1 à $p-1$,

forment une permutation de tous les éléments non nuls de $\text{CG}(p)$.

Soit un générateur y de $\text{CG}(p)$. Evaluons le rang du nombre $y^i \pmod{p}$ en

20 fonction de i et de $p-1$. Lorsque i est premier avec $p-1$, c'est $p-1$. Lorsque i

divise $p-1$, c'est $(p-1)/i$. Dans tous les cas, c'est $(p-1)/\text{pgcd}(p-1, i)$.

Par définition, la fonction d'Euler $\varphi(n)$ est le nombre de nombres plus petits

que n et premiers avec n . Dans $\text{CG}(p)$, il y a $\varphi(p-1)$ générateurs.

A titre d'illustration, le rang fait bien comprendre les bases du RSA. Le

25 module n est le produit de f facteurs premiers p_1 à p_f avec $f \geq 2$. Pour chaque

facteur premier p_j de p_1 à p_f , l'exposant public e doit être premier avec p_j-1 .

Alors, la clé $\langle e, p_j \rangle$ respecte le rang des éléments de $\text{CG}(p_j)$: elle permute les

éléments de $\text{CG}(p_j)$; il existe un nombre d_j , généralement le plus petit

possible, tel que p_j-1 divise $e \times d_j-1$. La clé $\langle d_j, p_j \rangle$ inverse la permutation des éléments de $CG(p_j)$. Ces f permutations, une dans chaque corps $CG(p_i)$ à $CG(p_f)$, se traduisent dans l'anneau des entiers modulo n par la permutation RSA résumée par la clé publique $\langle e, n \rangle$. Il existe un nombre d , généralement
 5 le plus petit possible, tel que $\text{ppcm}(p_1-1, p_2-1, \dots, p_f-1)$ divise $d \times e-1$. Pour chaque facteur premier p_i de p_1 à p_f , on a $d_j \equiv d \pmod{p_j-1}$. La permutation RSA résumée par la clé publique $\langle e, n \rangle$ est inversée par la clé privée $\langle d, n \rangle$.

Carrés dans $CG(p)$ — Définissons un nombre t tel que $p-1$ est divisible par 2^t , mais pas par 2^{t+1} . Chaque grand nombre premier figure dans une et
 10 une seule catégorie : $t=1$, $t=2$, $t=3$, $t=4$, et ainsi de suite. Si l'on considère un assez grand nombre de nombres premiers successifs, environ un sur deux figure dans la première catégorie où p est congru à 3 (mod 4), un sur quatre dans la deuxième où p est congru à 5 (mod 8), un sur huit dans la troisième où p est congru à 9 (mod 16), un sur seize dans la
 15 quatrième où p est congru à 17 (mod 32), et ainsi de suite ; en moyenne, un sur 2^t figure dans la t -ième catégorie où p est congru à $2^t+1 \pmod{2^{t+1}}$.

Parce que les nombres x et $p-x$ ont le même carré dans $CG(p)$, la clé $\langle 2, p \rangle$ ne permute pas $CG(p)$. La fonction « élever au carré » dans $CG(p)$ peut se représenter par un graphe orienté où chaque élément non nul du corps
 20 trouve sa place. Analysons la structure du graphe en branches et en cycles selon la parité du rang de chaque élément.

- L'élément nul est fixe. C'est 0. Le rang n'est pas défini pour l'élément nul auquel aucun autre élément ne se rattache ; l'élément nul est isolé.
- L'élément unité est fixe. C'est 1, le seul élément de rang 1. Toutes les
 25 racines de l'unité dans $CG(p)$ se trouvent dans la branche se rattachant à 1. Soit y un résidu non quadratique de $CG(p)$, n'importe lequel ; la clé $\langle (p-1)/2^t, p \rangle$ transforme y en une racine 2^{t-1} -ième primitive de -1 notée par b ; en effet, on a $y^{(p-1)/2} \equiv -1 \pmod{p}$. Par conséquent, dans $CG(p)$, les puissances de b pour les exposants de 1 à 2^{t-1} sont les 2^{t-1} racines de

l'unité autres que 1 : elles composent la branche se rattachant à 1.

- Le carré de tout élément de rang pair est un autre élément dont le rang est divisé par deux. Par conséquent, chaque élément de rang pair se place dans une branche ; chaque branche comporte un nombre de rang divisible par deux mais pas par quatre, puis, si $t \geq 2$, deux nombres de rang divisible par quatre mais pas par huit, puis, si $t \geq 3$, quatre nombres de rang divisible par huit mais pas par seize, puis, si $t \geq 4$, huit nombres de rang divisible par seize mais pas par 32, et ainsi de suite. Toutes les branches sont semblables à la branche rattachée à 1 ; les 2^{t-1} feuilles de chaque branche sont des résidus non quadratiques ; chaque branche comporte 2^{t-1} éléments et se rattache à un élément de rang impair ; il y a $(p-1)/2^t$ branches qui ont toutes la même longueur t .
- Le carré de tout élément de rang impair autre que l'élément unité est un autre élément ayant le même rang. La clé $\langle 2, p \rangle$ permute l'ensemble des $(p-1)/2^t$ éléments de rang impair. La permutation se décompose en cycles de permutation. Le nombre de cycles dépend de la factorisation de $(p-1)/2^t$. Pour chaque diviseur p' de $(p-1)/2^t$, il y a un cycle comportant les $\phi(p')$ éléments de rang p' . Rappelons que par définition, la fonction d'Euler $\phi(p')$ est le nombre de nombres plus petits que p' et premiers avec p' . Par exemple lorsque $p' = (p-1)/2^t$ est premier, les $p'-1$ nombres de rang p' forment un grand cycle de permutation.

Les figures 1A à 1D illustrent chacune un fragment de graphe pour p congru respectivement à 3 (mod 4), 5 (mod 8), 9 (mod 16) et 17 (mod 32).

- Les feuilles sur les branches sont représentées par des ronds blancs ; ce sont des résidus non quadratiques.
- Les nœuds dans les branches sont représentés par des ronds gris ; ce sont des éléments quadratiques de rang pair.
- Les nœuds dans les cycles sont représentés par des ronds noirs ; ce sont des éléments quadratiques de rang impair.

Racines carrées dans $CG(p)$ — Sachant que a est un résidu quadratique de $CG(p)$, voyons comment calculer une solution à l'équation $x^2 \equiv a \pmod{p}$, c'est-à-dire « prendre une racine carrée » dans $CG(p)$. Il y a bien sûr plusieurs façons d'obtenir le même résultat : on pourra consulter les pages

5 31 à 36 du livre de Henri Cohen, *a Course in Computational Algebraic Number Theory*, publié en 1993 par Springer à Berlin comme volume 138 de la série *Graduate Texts in Mathematics* (GTM 138).

Le nombre $s = (p-1+2^t)/2^{t+1}$ donne une clé $\langle s, p \rangle$ qui vaut :

$\langle (p+1)/4, p \rangle$ lorsque p est congru à 3 (mod 4),

10 $\langle (p+3)/8, p \rangle$ lorsque p est congru à 5 (mod 8),

$\langle (p+7)/16, p \rangle$ lorsque p est congru à 9 (mod 16),

$\langle (p+15)/32, p \rangle$ lorsque p est congru à 17 (mod 32),

et ainsi de suite.

- La clé $\langle s, p \rangle$ transforme tout élément d'un cycle en l'élément précédent dans le cycle. Lorsque a est de rang impair, c'est la solution de rang impair ; nous la nommons w . En effet, dans $CG(p)$, w^2/a vaut a élevé à la puissance $(2 \times (p-1+2^t)/2^{t+1}) - 1 = (p-1)/2^t$. L'autre solution est de rang pair ; c'est $p-w$.

- D'une manière générale, la clé $\langle s, p \rangle$ transforme tout résidu quadratique a en une première approximation de solution que nous nommons r . Puisque a est un résidu quadratique, la clé $\langle 2^{t-1}, p \rangle$ transforme certainement r^2/a en 1. Pour se rapprocher d'une racine carrée de a , élevons r^2/a à la puissance $2^{t-2} \pmod{p}$ pour obtenir +1 ou -1. La nouvelle approximation reste r si le résultat est +1 ou bien devient $b \times r \pmod{p}$ si le résultat est -1, sachant que b désigne n'importe quelle racine 2^t -ième primitive de 1 dans le corps $CG(p)$. Par conséquent, la clé $\langle 2^{t-2}, p \rangle$ transforme la nouvelle approximation en 1. On peut encore se rapprocher en utilisant la clé $\langle 2^{t-3}, p \rangle$ et en multipliant par $b^2 \pmod{p}$ s'il le faut, et ainsi de suite.

L'algorithme suivant résout l'équation. Il utilise les nombres a, b, p, r et t définis ci-dessus et deux variables : c représente les corrections successives

et w les approximations successives. Au début de l'algorithme, $c = b$ et $w = r$. A l'issue du calcul, les deux solutions sont w et $p-w$.

Pour i allant de $t-2$ à 1, répéter la séquence suivante :

- Appliquer la clé $\langle 2^i, p \rangle$ au nombre $w^2/a \pmod{p}$ pour obtenir $+1$ ou -1 .

5 - Lorsque l'on obtient -1 , remplacer w par $w \times c \pmod{p}$.

- Remplacer c par $c^2 \pmod{p}$.

Applicabilité des principes — Par définition, nous disons qu'un paramètre k , un nombre de base g et un facteur premier p sont compatibles lorsque l'équation $x^v \equiv g^2 \pmod{p}$ où l'exposant v vaut 2^k a des solutions en x dans le corps $\text{CG}(p)$. Les nombres k et g sont petits et plus grands que 1. Le nombre p est un grand nombre premier.

- Lorsque $t = 1$, c'est-à-dire $p \equiv 3 \pmod{4}$, l'équation a deux solutions.

15 - Lorsque $t = 2$, c'est-à-dire $p \equiv 5 \pmod{8}$, selon le symbole de Legendre de g par rapport à p , l'équation a quatre solutions si $(g|p) = +1$; elle n'a pas de solution si $(g|p) = -1$.

- Lorsque $t > 2$, c'est-à-dire $p \equiv 1 \pmod{8}$, soit u le nombre tel que 2^u divise le rang du nombre public $G = g^2$ par rapport à p , mais que 2^{u+1} ne le divise pas ; par conséquent, u est égal à l'un des nombres de 0 à $t-1$. L'équation n'a aucune solution si $u > 0$ et $k+u > t$; elle a 2^k solutions si $k+u \leq t$; elle a 2^t solutions si $u = 0$ et $k > t$.

Il y a donc deux types de compatibilité selon que G est dans un cycle ou bien en position appropriée dans une branche.

- Lorsque G est dans un cycle, c'est-à-dire $u = 0$ quelle que soit la valeur de k , il y a une solution de rang impair dans le cycle et des solutions de rang pair disséminées dans $\alpha = \min(k, t)$ branches consécutives
25 rattachées au cycle, soit 2^α solutions en tout. La figure 2A illustre ce cas avec $k \geq t = 3$, c'est-à-dire un facteur premier congru à 9 (mod 16), ce qui impose $u = 0$.

- Lorsque G est en position appropriée dans une branche, c'est-à-dire

$u > 0$ et $u+k \leq t$, il y a 2^k solutions, toutes de rang pair et dans la branche. La figure 2B illustre ce cas.

Etant donné un paramètre k , il y a donc deux types de facteurs premiers selon que la valeur de t est inférieure à k ou bien supérieure ou égale à k .

- 5 - Pour tout facteur premier p_j tel que $t < k$, chaque G_i doit être dans un cycle et il n'y a pas de solution dans la branche rattachée à G_i . Définissons un nombre $\Delta_{i,j}$ qui vaut +1 ou -1 selon que g_i ou $-g_i$ est dans le cycle. Il n'y a pas de choix pour aucun des m nombres $\Delta_{1,j}$ à $\Delta_{m,j}$. La figure 3A illustre un cas $t < k$: G_i est dans un cycle avec un facteur premier p_j congru à 9 (mod 16), c'est-à-dire, $u = 0$, $t = 3$ avec $k > 3$.
- 10 - Pour tout facteur premier p_j tel que $t \geq k$, chaque G_i doit être tel que $u+k \leq t$, c'est-à-dire, ou bien dans un cycle avec $u = 0$ ou bien en position appropriée dans une branche avec $1 \leq u \leq t-k$. Définissons un nombre $\Delta_{i,j}$ qui vaut +1 ou -1 selon que $Q_{i,j}$ se trouve dans la partie de
- 15 graphe rattachée à g_i ou à $-g_i$. Il y a le choix pour chacun des m nombres $\Delta_{1,j}$ à $\Delta_{m,j}$; chaque nombre $\Delta_{i,j}$ peut être individuellement basculé d'une valeur à l'autre. La figure 3B illustre un cas $t \geq k$: G_i est dans une branche avec un facteur premier p_j congru à 17 (mod 32), c'est-à-dire, $u = 1$, $t = 4$ avec $k = 3$.

20 Chaque jeu de f composantes $\{\Delta_{i,1} \dots \Delta_{i,f}\}$ est une racine carrée de l'unité dans $CG(p_j)$. Cette racine est triviale ou pas selon que les f composantes sont égales ou pas ; nous disons alors que le jeu de f composantes est constant ou variable, ce qui traduit le fait que le nombre q_i est trivial ou pas. Par conséquent, lorsqu'un nombre q_i est non trivial, le jeu de f composantes

25 $\{\Delta_{i,1} \dots \Delta_{i,f}\}$ résume une décomposition du module. Il est donc possible de tester les principes avant de calculer les composantes privées $Q_{i,j}$.

- Lorsqu'un nombre public G_i est dans un cycle pour un facteur premier p_j , le nombre $\Delta_{i,j}$ vaut +1 ou -1 selon que g_i ou $-g_i$ est dans le cycle. Lorsque $p_j \equiv 3 \pmod{4}$, c'est le symbole de Legendre : $\Delta_{i,j} = (g_i|p_j)$.

- Lorsqu'un nombre public G_i est en position appropriée dans une branche pour un facteur premier p_j , on peut déterminer la valeur à donner à Δ_{ij} avant de calculer la composante privée Q_{ij} .

Production de jeux de clés — Etant donné un paramètre k , il y a deux stratégies.

- Ou bien le générateur demande f facteurs premiers afin de déterminer m nombres de base. Les premiers nombres premiers : 2, 3, 5, 7, ... sont examinés pour évaluer leur compatibilité avec chacun des f grands facteurs premiers p_1 à p_f . Bien que $g = 2$ ne soit pas compatible avec $p \equiv 5 \pmod{8}$, 2 peut entrer dans la composition d'un nombre de base. En effet, lorsque deux nombres sont en position similaire dans une branche, leur produit est plus près du cycle, tout comme un carré rapproche du cycle. On peut ainsi obtenir un nombre de base en composant des nombres qui individuellement ne conviennent pas.
- Ou bien le générateur demande m nombres de base et des caractéristiques du module telle qu'une taille en bits (par exemple, 512, 768, 1024, 1536, 2048) et un nombre de bits successifs à 1 en poids forts (par exemple, 1, 8, 16, 24, 32) afin de déterminer $f \geq 2$ facteurs premiers. Notés par g_1, g_2, \dots, g_m , les nombres de base figurent généralement parmi les premiers nombres premiers : 2, 3, 5, 7, 11, ... ou bien ce sont des combinaisons des premiers nombres premiers. Faute d'indication contraire, ce sont les m premiers nombres premiers : $g_1 = 2$, $g_2 = 3$, $g_3 = 5$, $g_4 = 7$, ... Notons que $p \equiv 5 \pmod{8}$ n'est pas compatible avec $g = 2$. Le module n sera le produit de f facteurs premiers de tailles voisines, à savoir la taille assignée au module divisée par f .

Premier principe — Le paramètre k , chaque facteur premier p allant de p_1 à p_f et chaque nombre de base g allant de g_1 à g_m doivent être compatibles. Définissons un nombre h tel que 2^h divise le rang de g par rapport à p , alors que 2^{h+1} ne le divise pas. Pour calculer le nombre h , la procédure suivante

utilise le symbole de Legendre $(g|p)$ et un nombre b , racine 2^t -ième primitive de l'unité dans $CG(p)$.

- Si $(g|p) = +1$ avec $t = 1$, retourner « $h = 0$ ».

- Si $(g|p) = +1$ avec $t > 1$, appliquer la clé $\langle (p-1+2^t)/2^{t+1}, p \rangle$ à G pour obtenir un résultat appelé w .

- Si $w = +g$, retourner « $h = 0$ ».

- Si $w = p-g$, retourner « $h = 1$ ».

- Sinon, mettre c à b et pour i allant de $t-1$ à 2 ,

- appliquer la clé $\langle 2^i, p \rangle$ à $w/g \pmod{p}$ pour obtenir ± 1 ,

- si -1 , mettre h à i et remplacer w par $w \times c \pmod{p}$,

- remplacer c par $c^2 \pmod{p}$.

- Retourner « valeur de h de 2 à $t-1$ ».

- Si $(g|p) = -1$, retourner « $h = t$ ».

Rappelons que k , g et p sont incompatibles lorsque $u > 0$ avec $k+u > t$; ils sont compatibles lorsque $h = 0$ ou 1 , quelle que soit la valeur de k , et également lorsque $h > 1$ avec $k+h \leq t+1$.

Second principe — Les trois procédures suivantes correspondent à différentes implémentations du second principe. Dans certaines implémentations, le second principe peut être renforcé au point d'exiger que chaque nombre q_1 à q_m soit non trivial. Le rôle des nombres de base est alors équilibré; le fait d'équilibrer ou pas le second principe a un effet sur certains aspects de démonstration de la sécurité du schéma. Enfin, lorsqu'il y a $f > 2$ facteurs premiers distincts, parmi les m nombres $\{q_1 \dots q_m\}$, on peut exiger qu'il y ait au moins un sous ensemble de $f-1$ nombres indépendants.

Les trois procédures utilisent $m \times f$ nombres δ_{ij} définis comme suit.

- Lorsque p_j est tel que $t < k$, pour i allant de 1 à m , $\delta_{ij} = \Delta_{ij}$, c'est-à-dire $+1$ si $h_{ij} = 0$ et -1 si $h_{ij} = 1$.

- Lorsque p_j est tel que $t \geq k$, pour i allant de 1 à m , $\delta_{ij} = 0$, ce qui indique que $\Delta_{1,j}$ à $\Delta_{m,j}$ peuvent être choisis en fonction du deuxième principe.

Une première procédure vérifie qu'au moins un jeu $\{\delta_{i,1} \dots \delta_{i,f}\}$ est variable ou nul, c'est-à-dire qu'au moins un nombre q_1 à q_m est non trivial ou peut être choisi non trivial.

- Pour i allant de 1 à m et j allant de 1 à f ,
 - si $\delta_{i,j} = 0$ ou $\neq \delta_{i,1}$, retourner « succès ».
- Retourner « échec ».

Une deuxième procédure vérifie que chaque jeu $\{\delta_{i,1} \dots \delta_{i,f}\}$ est variable ou nul, c'est-à-dire que chaque nombre q_1 à q_m est non trivial ou peut être choisi non trivial.

- Pour i allant de 1 à m ,
 - pour j allant de 1 à f ,
 - si $\delta_{i,j} = 0$ ou $\neq \delta_{i,1}$, passer à la valeur suivante de j .
 - Retourner « échec ».
- Retourner « succès ».

Une troisième procédure vérifie que pour chaque paire de facteurs premiers p_{j_1} et p_{j_2} avec $1 \leq j_1 < j_2 \leq f$, il y a au moins un jeu $\{\delta_{i,1} \dots \delta_{i,f}\}$ où δ_{i,j_1} est nul ou différent de δ_{i,j_2} . Elle échoue manifestement lorsque m est plus petit que $f-1$. Lorsqu'elle réussit, parmi les m nombres q_1 à q_m , il y a au moins un ensemble de $f-1$ nombres indépendants par rapport aux f facteurs premiers.

- Pour j_1 allant de 1 à $f-1$ et pour j_2 allant de j_1+1 à f ,
 - pour i allant de 1 à m ,
 - si $\delta_{i,j_1} = 0$ ou $\neq \delta_{i,j_2}$, passer aux valeurs suivantes de j_1 et j_2 .
 - Retourner « échec ».
- Retourner « succès ».

Lorsqu'une procédure échoue, le générateur de jeux de clés GQ2 suit sa stratégie parmi les deux stratégies possibles :

- changer l'un des m nombres de base en gardant les f facteurs premiers,
- changer l'un des f facteurs premiers en gardant les m nombres de base.

Troisième principe — La procédure suivante détermine si le jeu de clés

GQ2 généralisées en cours de production ou déjà produit est

- un jeu de clés GQ2 élémentaires, c'est-à-dire que les $2 \times m$ nombres $\pm g_1$ à $\pm g_m$ sont tous des résidus non quadratiques,
- ou bien, un jeu de clés GQ2 complémentaires, c'est-à-dire que parmi

La procédure utilise les deux symboles de Legendre $(g_i | p_j)$ et $(-g_i | p_j)$ pour i allant de 1 à m et pour j allant de 1 à f .

- Pour i allant de 1 à m ,
 - pour j allant de 1 à f ,
 - si $(g_i | p_j) = -1$, passer à la valeur suivante de i .
 - Retourner « jeu de clés GQ2 complémentaires ».
 - pour j allant de 1 à f ,
 - si $(-g_i | p_j) = -1$, passer à la valeur suivante de i .
 - Retourner « jeu de clés GQ2 complémentaires ».
 - Retourner « jeu de clés GQ2 élémentaires ».

Composantes privées — Pour une équation de type direct : $x^v \equiv g_i^2 \pmod{p_j}$, les calculs suivants établissent toutes les valeurs possibles de la composante privée Q_{ij} . Les deux cas les plus simples et les plus courants, c'est-à-dire $t = 1$ et $t = 2$, sont suivis par le cas plus complexe, c'est-à-dire $t > 2$.

Pour $t = 1$, c'est-à-dire $p_j \equiv 3 \pmod{4}$, la clé $\langle (p_j+1)/4, p_j \rangle$ donne la racine carrée quadratique de n'importe quel résidu quadratique dans $CG(p_j)$. On en déduit un nombre $s_j \equiv ((p_j+1)/4)^k \pmod{(p_j-1)/2}$, ce qui donne une clé $\langle s_j, p_j \rangle$ transformant G_i en $w \equiv G_i^{s_j} \pmod{p_j}$. Q_{ij} est égal à w ou bien à $p_j - w$.

Pour $t = 2$, c'est-à-dire $p_j \equiv 5 \pmod{8}$, la clé $\langle (p_j+3)/8, p_j \rangle$ donne la racine carrée de rang impair de n'importe quel élément de rang impair dans $CG(p_j)$. On en déduit un nombre $s_j \equiv ((p_j+3)/8)^k \pmod{(p_j-1)/4}$, ce qui donne une clé $\langle s_j, p_j \rangle$ transformant G_i en $w \equiv G_i^{s_j} \pmod{p_j}$. Remarquons que $z \equiv 2^{(p_j-1)/4} \pmod{p_j}$ est une racine carrée de -1 parce que 2 est un résidu non quadratique dans $CG(p_j)$. Q_{ij} est égal à w ou bien à $p_j - w$ ou bien encore à

$w' \equiv w \times z \pmod{p_j}$ ou bien à $p_j - w'$.

Pour $p_j \equiv 2^t + 1 \pmod{2^{t+1}}$ avec $t > 2$, la clé $\langle (p_j - 1 + 2^t)/2^{t+1}, p_j \rangle$ donne la racine carrée de rang impair de n'importe quel élément de rang impair. Le test de compatibilité entre k , g et p a donné la valeur de h , puis celle de u .

- 5 - Lorsque G_i est dans un cycle ($u = 0$, quelle que soit la valeur de k), on établit un nombre $s_j \equiv ((p_j - 1 + 2^t)/2^{t+1})^k \pmod{(p_j - 1)/2^t}$. La clé $\langle s_j, p_j \rangle$ transforme G_i en la solution de rang impair $w \equiv G_i^{s_j} \pmod{p_j}$. Il y des solutions de rang pair réparties dans $\min(k, t)$ branches consécutives rattachées au cycle, disons dans α branches. Q_{ij} est égal au produit de w
- 10 par n'importe laquelle des racines 2^α -ièmes de l'unité dans $CG(p_j)$.
- Lorsque G_i est en position appropriée dans une branche ($u > 0$, $u + k \leq t$), toutes les solutions sont dans la même branche que G_i , branche rattachée à un cycle par la puissance 2^u -ième du nombre G_i . On établit un nombre $s_j \equiv ((p_j - 1 + 2^t)/2^{t+1})^{k+u} \pmod{(p_j - 1)/2^t}$. La clé $\langle s_j, p_j \rangle$ transforme la puissance
- 15 2^u -ième de G_i en un nombre de rang impair w . L'ensemble des produits de w par les racines 2^{k+u} -ièmes primitives de l'unité dans $CG(p_j)$ comprend les 2^k valeurs de Q_{ij} .

Lorsque p_j est tel que $t \geq k$, le nombre b_j étant une racine 2^t -ième primitive de l'unité dans $CG(p_j)$, la puissance 2^{t-u} -ième de b_j dans $CG(p_j)$ existe ; c'est

20 une racine 2^k -ième primitive de l'unité. Multiplier Q_{ij} par une racine 2^k -ième primitive de l'unité permet de basculer la valeur du nombre Δ_{ij} .

Pour une équation de type inverse : $1 \equiv x^v \times g_i^2 \pmod{p_j}$, il suffit de remplacer le nombre s_j par $((p_j - 1)/2^t) - s_j$ dans la clé $\langle s_j, p_j \rangle$, ce qui revient à inverser la valeur de Q_{ij} dans $CG(p_j)$.

25 **Exemple de jeu de clés à deux facteurs premiers congrus à 5 (mod 8)**

$p_1 = \text{E6C83BF428689AF8C35E07EDD06F9B39A659829A58B79CD894C}$
 $435C95F32BF25$

$p_2 = \text{11BF8A68A0817BFCC00F15731C8B70CEF9204A34133A0DEF862}$
 $829B2EEA74873D$

$n = p_1 \times p_2 = \text{FFFF8263434F173D0F2E76B32D904F56F4A5A6A50008C43}$
 $\text{D32B650E9AB9AAD2EB713CD4F9A97C4DBDA3828A3954F296458D5}$
 $\text{F42C0126F5BD6B05478BE0A80ED1}$

Voici les symboles de Legendre des tout premiers nombres premiers.

5 $(2 | p_1) = -1; (3 | p_1) = -1; (5 | p_1) = +1; (7 | p_1) = -1;$
 $(11 | p_1) = +1; (13 | p_1) = -1; (17 | p_1) = +1;$

Dans $\text{CG}(p_1)$, le rang est impair pour $-5, -11$ et 17 .

$(2 | p_2) = -1; (3 | p_2) = +1; (5 | p_2) = +1; (7 | p_2) = +1;$
 $(11 | p_2) = +1; (13 | p_2) = -1; (17 | p_2) = -1;$

10 Dans $\text{CG}(p_2)$, le rang est impair pour $3, -5, 7$ et 11 .

La fonction de Carmichael est $\lambda(n) = \text{ppcm}((p_1-1)/4, (p_2-1)/4)$.

$\lambda(n) = \text{33331A13DA4304A5CFD617BD6F834311642121543334F40C3D5}$
 $\text{7A9C8558555D5BDAA2EF6AED17B9E3794F51A65A1B37239B18FA9}$
 $\text{B0F618627D8C7E1D8499C1B}$

15 Avec $k = 9$, on utilise le nombre $\sigma \equiv \lambda(n) - ((1+\lambda(n))/2)^9 \pmod{\lambda(n)}$ comme exposant privé, de façon à utiliser des équations génériques de type inverse.

$\sigma = \text{01E66577BC997CAC273671E187A35EFD25373ABC9FE6770E7446}$
 $\text{C0CCEF2C72AF6E89D0BE277CC6165F1007187AC58028BD2416D4CC}$
 $\text{1121E7A7A8B6AE186BB4B0}$

20 Les nombres $2, 3, 7, 13$ et 17 ne conviennent pas comme nombre de base.

La clé $\langle \sigma, n \rangle$ transforme $g_1 = 5$ en un nombre privé Q_1 qui ne révèle pas de décomposition. En effet, dans les deux corps, -5 est sur un cycle.

$Q_1 = \text{818C23AF3DE333FAECE88A71C4591A70553F91D6C0DD5538EC}$
 $\text{0F2AAAF909B5BDAD491FD8BF13F18E3DA3774CCE19D0097BC4BD4}$
 $\text{7C5D6E0E7EBF6D89FE3DC5176C}$

25

La clé $\langle \sigma, n \rangle$ transforme $g_2 = 11$ en un nombre privé Q_2 qui révèle une décomposition. En effet, 11 n'est pas en même position dans les deux corps.

$Q_2 = \text{25F9AFDF177993BE8652CE6E2C728AF31B6D66154D3935AC535}$
 $\text{196B07C19080DC962E4E86ACF40D01FDC454F2565454F290050DA05}$

2089EEC96A1B7DEB92CCA7

La clé $\langle \sigma, n \rangle$ transforme $g_3 = 21 = 3 \times 7$ en un nombre privé Q_3 qui révèle une décomposition.

$Q_3 = 78A8A2F30FEB4A5233BC05541AF7B684C2406415EA1DD67D18$
 $A0459A1254121E95D5CAD8A1FE3ECFE0685C96CC7EE86167D99532$
 $B3A96B6BF9D93CAF8D4F6AF0$

La clé $\langle \sigma, n \rangle$ transforme $g_4 = 26 = 2 \times 13$ en un nombre privé Q_4 qui révèle une décomposition.

$Q_4 = 6F1748A6280A200C38824CA34C939F97DD2941DAD300030E481$
 $B738C62BF8C673731514D1978AF5655FE493D659514A6CE897AB76C$
 $01E50B5488C5DAD12332E5$

La clé privée peut encore se représenter par les deux facteurs premiers, le paramètre des restes chinois et huit composantes privées.

$\alpha \equiv (p_2 \pmod{p_1})^{-1} \pmod{p_1} = ADE4E77B703F5FDEAC5B9AAE825D649$
 $E06692D15FBF0DF737B115DC4D012FD1D$

$Q_{1,1} \equiv Q_1 \pmod{p_1} = 7751A9EE18A8F5CE44AD73D613A4F465E06C6F9$
 $AF4D229949C74DD6C18D76FAF$

$Q_{1,2} \equiv Q_1 \pmod{p_2} = A9EB5FA1B2A981AA64CF88C382923DB64376F5F$
 $D48152C08EEB6114F31B7665F$

$Q_{2,1} \equiv Q_2 \pmod{p_1} = D5A7D33C5FB75A033F2F0E8B20274B957FA3400$
 $4ABB2C2AC1CA3F5320C5A9049$

$Q_{2,2} \equiv Q_2 \pmod{p_2} = 76C9F5EFD066C73A2B5CE9758DB512DFC011F5B$
 $5AF7DA8D39A961CC876F2DD8F$

$Q_{3,1} \equiv Q_3 \pmod{p_1} = 2FEC0DC2DCA5BA7290B27BC8CC85C938A514B$
 $8F5CFD55820A174FB5E6DF7B883$

$Q_{3,2} \equiv Q_3 \pmod{p_2} = 010D488E6B0A38A1CC406CEE0D55DE59013389D$
 $8549DE493413F34604A160C1369$

$Q_{4,1} \equiv Q_4 \pmod{p_1} = A2B32026B6F82B6959566FADD9517DB8ED85246$
 $52145EE159DF3DC0C61FE3617$

$Q_{4,2} \equiv Q_4 \pmod{p_2} = 011A3BB9B607F0BD71BBE25F52B305C224899E5$
 $F1F8CDC2FE0D8F9FF62B3C9860F$

Polymorphisme de la clé privée GQ2 — Les diverses représentations possibles de la clé privée GQ2 s'avèrent équivalentes : elles se ramènent toutes à la connaissance de la factorisation du module n qui est la véritable clé privée GQ2. La représentation de la clé privée GQ2 a un effet sur le déroulement des calculs au sein de l'entité qui prouve, pas au sein de l'entité qui contrôle. Voici les trois principales représentations possibles de la clé privée GQ2. 1) La représentation classique des clés privées GQ consiste à stocker m nombres privés Q_i et la clé publique de vérification $\langle v, n \rangle$; pour les schémas GQ2, cette représentation est concurrencée par les deux suivantes. 2) La représentation optimale en termes de charges de travail consiste à stocker le paramètre k , les f facteurs premiers p_j , $m \times f$ composantes privées Q_{ij} et $f-1$ paramètres des restes chinois. 3) La représentation optimale en termes de taille de clé privée consiste à stocker le paramètre k , les m nombres de base g_i et les f facteurs premiers p_j , puis, à commencer chaque utilisation en établissant ou bien m nombres privés Q_i et le module n pour se ramener à la première représentation, ou bien $m \times f$ composantes privées Q_{ij} et $f-1$ paramètres des restes chinois pour se ramener à la seconde.

Parce que la sécurité du mécanisme d'authentification dynamique ou de signature numérique équivaut à la connaissance d'une décomposition du module, les schémas GQ2 ne permettent pas de distinguer simplement deux entités utilisant le même module. Généralement, chaque entité qui prouve dispose de son propre module GQ2. Toutefois, on peut spécifier des modules GQ2 à quatre facteurs premiers dont deux sont connus d'une entité et les deux autres d'une autre.

Authentification dynamique — Le mécanisme d'authentification dynamique est destiné à prouver à une entité appelée **contrôleur** l'authenticité

d'une autre entité appelée **démonstrateur** ainsi que l'authenticité d'un éventuel message associé M , de sorte que le contrôleur s'assure qu'il s'agit bien du démonstrateur et éventuellement que lui et le démonstrateur parlent bien du même message M . Le message associé M est optionnel, ce qui signifie qu'il peut être vide.

Le mécanisme d'authentification dynamique est une séquence de quatre actes : un acte d'engagement, un acte de défi, un acte de réponse et un acte de contrôle. Le démonstrateur joue les actes d'engagement et de réponse. Le contrôleur joue les actes de défi et de contrôle.

Au sein du démonstrateur, on peut isoler un témoin, de manière à isoler les paramètres et les fonctions les plus sensibles du démonstrateur, c'est-à-dire, la production des engagements et des réponses. Le témoin dispose du paramètre k et de la clé privée GQ2, c'est-à-dire, de la factorisation du module n selon l'une des trois représentations évoquées ci-dessus : • les f facteurs premiers et les m nombres de base, • les $m \times f$ composantes privées, les f facteurs premiers et $f-1$ paramètres des restes chinois, • les m nombres privés et le module n .

Le témoin peut correspondre à une réalisation particulière, par exemple, • une carte à puce reliée à un PC formant ensemble le démonstrateur, ou encore, • des programmes particulièrement protégés au sein d'un PC, ou encore, • des programmes particulièrement protégés au sein d'une carte à puce. Le témoin ainsi isolé est semblable au témoin défini ci-après au sein du signataire. A chaque exécution du mécanisme, le témoin produit un ou plusieurs engagements R , puis, autant de réponses D à autant de défis d . Chaque ensemble $\{R, d, D\}$ constitue un **triplet GQ2**.

Outre qu'il comprend le témoin, le démonstrateur dispose également, le cas échéant, d'une fonction de hachage et d'un message M .

Le contrôleur dispose du module n , par exemple, à partir d'un annuaire de clés publiques ou encore à partir d'un certificat de clés publique ; le cas

échéant, il dispose également de la même fonction de hachage et d'un
 message M' . Les paramètres publics GQ2, à savoir les nombres k , m et g_1 à
 g_m peuvent être donnés au contrôleur par le démonstrateur. Le contrôleur est
 apte à reconstituer un engagement R' à partir de n'importe quel défi d et de
 5 n'importe quelle réponse D . Les paramètres k et m renseignent le
 contrôleur. Faute d'indication contraire, les m nombres de base de g_1 à g_m
 sont les m premiers nombres premiers. Chaque défi d doit comporter m
 défis élémentaires notés de d_1 à d_m : un par nombre de base. Chaque défi
 élémentaire de d_1 à d_m est un nombre de 0 à $2^{k-1}-1$ (les nombres de $v/2$ à $v-1$
 10 ne sont pas utilisés). Typiquement, chaque défi est codé par m fois $k-1$ bits
 (et non pas m fois k bits). Par exemple, avec $k = 5$ et $m = 4$ nombres de base
 5, 11, 21 et 26, chaque défi comporte 16 bits transmis sur quatre quartets.
 Lorsque les $(k-1) \times m$ défis possibles sont également probables, le nombre
 $(k-1) \times m$ détermine la sécurité apportée par chaque triplet GQ2: un
 15 imposteur qui, par définition, ne connaît pas la factorisation du module n a
 exactement une chance de succès sur $2^{(k-1) \times m}$. Lorsque $(k-1) \times m$ vaut de 15 à
 20, un triplet suffit à assurer raisonnablement l'authentification dynamique.
 Pour atteindre n'importe quel niveau de sécurité, on peut produire des
 triplets en parallèle; on peut également en produire en séquence, c'est-à-
 20 dire, répéter l'exécution du mécanisme.

1) **L'acte d'engagement** comprend les opérations suivantes.

Lorsque le témoin n'utilise pas les restes chinois, il dispose du paramètre k ,
 des m nombres privés de Q_1 à Q_m et du module n ; il tire au hasard et en
 privé un ou plusieurs aléas r ($0 < r < n$); puis, par k élévations successives
 25 au carré (mod n), il transforme chaque aléa r en un engagement R .

$$R \equiv r^v \pmod{n}$$

Voici un exemple avec le jeu de clés précédent sans les restes chinois.

$r = 5E94B894AC24AF843131F437C1B1797EF562CFA53AB8AD426C1$
 $AC016F1C89CFDA13120719477C3E2FB4B4566088E10EF9C010E8F09$

C60D981512198126091996

$R = 6BBF9FFA5D509778D0F93AE074D36A07D95FFC38F70C8D7E330$
 $0EBF234FA0BC20A95152A8FB73DE81FAEE5BF4FD3EB7F5EE3E36D$
 $7068D083EF7C93F6FDDF673A$

- 5 Lorsque le témoin utilise les restes chinois, il dispose du paramètre k , des f facteurs premiers de p_1 à p_f de $f-1$ paramètres des restes chinois et des $m \times f$ composantes privées Q_{ij} ; il tire au hasard et en privé une ou plusieurs collections de f aléas : chaque collection comporte un aléa r_i par facteur premier p_i ($0 < r_i < p_i$); puis, par k élévations successives au carré (mod p_i),
 10 il transforme chaque aléa r_i en une composante d'engagement R_i .

$$R_i \equiv r_i^v \pmod{p_i}$$

Pour chaque collection de f composantes d'engagement, le témoin établit un engagement selon la technique des restes chinois. Il y a autant d'engagements que de collections d'aléas.

- 15 $R = \text{Restes Chinois}(R_1, R_2, \dots, R_f)$

Voici un exemple avec le jeu de clés précédent et avec les restes chinois.

$r_1 = 5C6D37F0E97083C8D120719475E080BBBF9F7392F11F3E244FDF0$
 $204E84D8CAE$

- 20 $R_1 = 3DDF516EE3945CB86D20D9C49E0DA4D42281D07A76074DD4FE$
 $C5C7C5E205DF66$

$r_2 = AC8F85034AC78112071947C457225E908E83A2621B0154ED15DB$
 $FCB9A4915AC3$

$R_2 = 01168CEC0F661EAA15157C2C287C6A5B34EE28F8EB4D8D34085$
 $8079BCAE4ECB016$

- 25 $R = \text{Restes Chinois}(R_1, R_2) = 0AE51D90CB4FDC3DC757C56E063C9ED8$
 $6BE153B71FC65F47C123C27F082BC3DD15273D4A923804718573F2F0$
 $5E991487D17DAE0AAB7DF0D0FFA23E0FE59F95F0$

Dans les deux cas, le démonstrateur transmet au contrôleur tout ou partie de chaque engagement R , ou bien, un code de hachage H obtenu en hachant

chaque engagement R et un message M .

2) L'acte de défi consiste à tirer au hasard un ou plusieurs défis d composés chacun de m défis élémentaires $d_1 \ d_2 \dots d_m$; chaque défi élémentaire d_i est l'un des nombres de 0 à $v/2-1$.

5

$$d = d_1 \ d_2 \dots d_m$$

Voici un défi pour les deux exemples, c'est-à-dire avec $k = 5$ et $m = 4$.

$$d_1 = 1011 = 11 = 'B'; d_2 = 0011 = 3; d_3 = 0110 = 6; d_4 = 1001 = 9,$$

$$d = d_1 \ || \ d_2 \ || \ d_3 \ || \ d_4 = 10110011 \ 01101001 = B3 \ 69$$

Le contrôleur transmet au démonstrateur chaque défi d .

10

3) L'acte de réponse comporte les opérations suivantes.

Lorsque le témoin n'utilise pas les restes chinois, il dispose du paramètre k , des m nombres privés de Q_1 à Q_m et du module n ; il calcule une ou plusieurs réponses D en utilisant chaque aléa r de l'acte d'engagement et les nombres privés selon les défis élémentaires.

15

$$D \equiv r \times Q_1^{d_1} \times Q_2^{d_2} \times \dots Q_m^{d_m} \pmod{n}$$

Voici la suite de l'exemple sans les restes chinois.

$D = 027E6E808425BF2B401FD00B15B642B1A8453BE8070D86C0A787$
 $0E6C1940F7A6996C2D871EBE611812532AC5875E0E116CC8BA648FD$
 $8E86BE0B2ABCC3CCBBBE4$

20

Lorsque le témoin utilise les restes chinois, il dispose du paramètre k , des f facteurs premiers de p_1 à p_f , de $f-1$ paramètres des restes chinois et des $m \times f$ composantes privées Q_{ij} ; il calcule une ou plusieurs collections de f composantes de réponse en utilisant chaque collection d'aléas de l'acte d'engagement : chaque collection de composantes de réponse comporte une

25

composante par facteur premier.

$$D_i \equiv r_i \times Q_{1,i}^{d_1} \times Q_{2,i}^{d_2} \times \dots Q_{m,i}^{d_m} \pmod{p_i}$$

Pour chaque collection de composantes de réponse, le témoin établit une réponse selon la technique des restes chinois. Il y a autant de réponses que de défis.

$$D = \text{Restes.Chinois}(D_1, D_2, \dots D_p)$$

Voici la suite de l'exemple avec les restes chinois.

$$D_1 = r_1 \times Q_{1,1}^{d_1} \times Q_{2,1}^{d_2} \times Q_{3,1}^{d_3} \times Q_{4,1}^{d_4} \pmod{p_1} =$$

C71F86F6FD8F955E2EE434BFA7706E38E5E715375BC2CD2029A4BD
572A9EDEE6

$$D_2 = r_2 \times Q_{1,2}^{d_1} \times Q_{2,2}^{d_2} \times Q_{3,2}^{d_3} \times Q_{4,2}^{d_4} \pmod{p_2} =$$

0BE022F4A20523F98E9F5DBEC0E10887902F3AA48C864A6C354693A
D0B59D85E

$$D = 90CE7EA43CB8EA89ABDD0C814FB72ADE74F02FE6F098ABB98$$

C8577A660B9CFCEAECB93BE1BCC356811BF12DD667E2270134C907
3B9418CA5EBF5191218D3FDB3

Dans les deux cas, le démonstrateur transmet chaque réponse D au contrôleur.

4) **L'acte de contrôle** consiste à contrôler que chaque triplet $\{R, d, D\}$ vérifie une équation du type suivant pour une valeur non nulle,

$$R \times \prod_{i=1}^m G_i^{d_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k} \times \prod_{i=1}^m G_i^{d_i} \pmod{n}$$

ou bien, à rétablir chaque engagement : aucun ne doit être nul.

$$R' \equiv D^{2^k} / \prod_{i=1}^m G_i^{d_i} \pmod{n} \quad \text{ou bien} \quad R' \equiv D^{2^k} \times \prod_{i=1}^m G_i^{d_i} \pmod{n}$$

Eventuellement, le contrôleur calcule ensuite un code de hachage H' en hachant chaque engagement rétabli R' et un message M' . L'authentification dynamique est réussie lorsque le contrôleur retrouve ainsi ce qu'il a reçu à l'issue de l'acte d'engagement, c'est-à-dire, tout ou partie de chaque engagement R , ou bien, le code de hachage H .

Par exemple, une séquence d'opérations élémentaires transforme la réponse D en un engagement R' . La séquence comprend k carrés $(\text{mod } n)$ séparés par $k-1$ divisions ou multiplications $(\text{mod } n)$ par des nombres de base. Pour la i ième division ou multiplication, qui s'effectue entre le i ième carré et le

$i+1$ ième carré, le i ième bit du défi élémentaire d_1 indique s'il faut utiliser g_1 , le i ième bit du défi élémentaire d_2 indique s'il faut utiliser g_2 , ... jusqu'au i ième bit du défi élémentaire d_m qui indique s'il faut utiliser g_m .

Voici la fin de l'exemple sans les restes chinois.

5 $D = 027E6E808425BF2B401FD00B15B642B1A8453BE8070D86C0A787$
 $0E6C1940F7A6996C2D871EBE611812532AC5875E0E116CC8BA648FD$
 $8E86BE0B2ABCC3CCBBBE4$

Elever au carré modulo n :

88BA681DD641D37D7A7D9818D0DBEA82174073997C6C32F7FCAB3
 10 $0380C4C6229B0706D1AF6EBD84617771C31B4243C2F0376CAF5DCE$
 $B644F098FAF3B1EB49B39$

Multiplier par 5 fois $26 = 130$, soit '82' modulo n :

6ECABA65A91C22431C413E4EC7C7B39FDE14C9782C94FD6FA3CA
 AD7AFE192B9440C1113CB8DBC45619595D263C1067D3D0A840FDE0
 15 $08B415028AB3520A6AD49D$

Elever au carré modulo n :

0236D25049A5217B13818B39AFB009E4D7D52B17486EBF844D64CF7
 5C4F652031041328B29EBF0829D54E3BD17DAD218174A01E6E3AA65
 0C6FD62CC274426607

20 Multiplier par 21, soit '15' modulo n :

2E7F40960A8BBF1899A06BBB6970CFC5B47C88E8F115B5DA594504
 A92834BA405559256A705ABAB6E7F6AE82F4F33BF9E91227F0ACFA
 4A052C91ABF389725E93

Elever au carré modulo n :

B802171179648AD687E672D3A32640E2493BA2E82D5DC87DBA2B2C
 C0325E7A71C50E8AE02E299EF868DD3FB916EBCBC0C5569B53D42
 DAD49C956D8572E1285B0

Multiplier par 5 fois 11 fois 21 = 1155, soit '483' modulo n :

3305560276310DEFEC1337EB5BB5810336FDB28E91B350D485B09188

E0C4F1D67E68E9590DB7F9F39C22BDB4533013625011248A8DC417C
667B419D27CB11F72

Elever au carré modulo n :

8871C494081ABD1AEB8656C38B9BAAB57DBA72A4BD4EF9029ECB
5 FFF540E55138C9F22923963151FD0753145DF70CE22E9D019990E41D
B6104005EEB7B1170559

Multiplier par 5 fois 11 fois 26 = 1430, soit '596' modulo n :

2CF5F76EEBF128A0701B56F837FF68F81A6A5D175D0AD67A14DAE
C6FB68C362B1DC0ADD6CFC004FF5EEACDF794563BB09A17045EC
10 FFF88F5136C7FBC825BC50C

Elever au carré modulo n :

6BBF9FFA5D509778D0F93AE074D36A07D95FFC38F70C8D7E3300EB
F234FA0BC20A95152A8FB73DE81FAEE5BF4FD3EB7F5EE3E36D706
8D083EF7C93F6FDDF673A

15 On retrouve bien l'engagement R . L'authentification est réussie.

Voici la fin de l'exemple avec les restes chinois.

$D = 90CE7EA43CB8EA89ABDD0C814FB72ADE74F02FE6F098ABB98$
C8577A660B9CFCEAECB93BE1BCC356811BF12DD667E2270134C907
3B9418CA5EBF5191218D3FDB3

20 Elever au carré modulo n :

770192532E9CED554A8690B88F16D013010C903172B266C1133B136E
BE3EB5F13B170DD41F4ABE14736ADD3A70DFA43121B6FC5560CD
D4B4845395763C792A68

Multiplier par 5 fois 26 = 130, soit '82' modulo n :

25 6EE9BEF9E52713004971ABB9FBC31145318E2A703C8A2FB3E144E77
86397CD8D1910E70FA86262DB771AD1565303AD6E4CC6E90AE3646
B461D3521420E240FD4

Elever au carré modulo n :

D9840D9A8E80002C4D0329FF97D7AD163D8FA98F6AF8FE2B2160B2

126CBBD7FC734E39F2C9A39983A426486BC477F20ED2CA59E664C23
CA0E04E84F2F0AD65340

Multiplier par 21, soit '15' modulo n :

D7DD7516383F78944F2C90116E1BEE0CCDC8D7CEC5D7D1795ED33
5 BFE8623DB3D2E5B6C5F62A56A2DF4845A94F32BF3CAC360C7782B
5941924BB4BE91F86BD85F

Elever au carré modulo n :

DD34020DD0804C0757F29A0CBBD7B46A1BAF949214F74FD7FE021B
626ADAFBAB5C3F1602095DA39D70270938AE362F2DAE0B91485531
10 0C7BCA328A4B2643DCCDF

Multiplier par 5 fois 11 fois 21 = 1155, soit '483' modulo n :

038EF55B4C826D189C6A48EFDD9DADBD2B63A7D675A0587C85596
18EA2D83DF552D24EAF6BE983FB4AFB3DE7D4D2545190F1B1F946
D327A4E9CA258C73A98F57

15 Elever au carré modulo n :

D1232F50E30BC6B7365CC2712E5CAE079E47B971DA03185B33E918E
E6E99252DB3573CC87C604B327E5B20C7AB920FDF142A8909DBBA1
C04A6227FF18241C9FE

Multiplier par 5 fois 11 fois 26 = 1430, soit '596' modulo n :

20 3CC768F12AEDFCD4662892B9174A21D1F0DD9127A54AB63C984019
BED9BF88247EF4CCB56D71E0FA30CFB0FF28B7CE45556F744C1FD7
51BFBCA040DC9CBAB744

Elever au carré modulo n :

0AE51D90CB4FDC3DC757C56E063C9ED86BE153B71FC65F47C123C
25 27F082BC3DD15273D4A923804718573F2F05E991487D17DAE0AAB7
DF0D0FFA23E0FE59F95F0

On retrouve bien l'engagement R . L'authentification est réussie.

Signature numérique

Le mécanisme de signature numérique permet à une entité appelée

signataire de produire des messages signés et à une entité appelée contrôleur de vérifier des messages signés. Le message M est une séquence binaire quelconque : il peut être vide. Le message M est signé en lui adjoignant un appendice de signature qui comprend un ou plusieurs engagements et / ou défis, ainsi que les réponses correspondantes.

Le contrôleur dispose du module n , par exemple, à partir d'un annuaire de clés publiques ou encore à partir d'un certificat de clés publique ; il dispose également de la même fonction de hachage. Les paramètres publics GQ2, à savoir les nombres k , m et g_1 à g_m peuvent être donnés au contrôleur par le démonstrateur, par exemple, en les mettant dans l'appendice de signature.

Les nombres k et m renseignent le contrôleur. D'une part, chaque défi élémentaire, de d_1 à d_m , est un nombre de 0 à $2^{k-1}-1$ (les nombres $v/2$ à $v-1$ ne sont pas utilisés). D'autre part, chaque défi d doit comporter m défis élémentaires notés de d_1 à d_m , autant que de nombres de base. En outre, faute d'indication contraire, les m nombres de base, de g_1 à g_m , sont les m premiers nombres premiers. Avec $(k-1) \times m$ valant de 15 à 20, on peut signer avec quatre triplets GQ2 produits en parallèle ; avec $(k-1) \times m$ valant 60 ou plus, on peut signer avec un seul triplet GQ2. Par exemple, avec $k=9$ et $m=8$, un seul triplet GQ2 suffit ; chaque défi comporte huit octets et les nombres de base sont 2, 3, 5, 7, 11, 13, 17 et 19.

L'opération de signature est une séquence de trois actes : un acte d'engagement, un acte de défi et un acte de réponse. Chaque acte produit un ou plusieurs triplets GQ2 comprenant chacun : un engagement R ($\neq 0$), un défi d composé de m défis élémentaires notés par d_1, d_2, \dots, d_m et une réponse D ($\neq 0$).

Le signataire dispose d'une fonction de hachage, du paramètre k et de la clé privée GQ2, c'est-à-dire, de la factorisation du module n selon l'une des trois représentations évoquées ci-dessus. **Au sein du signataire, on peut isoler un témoin qui exécute les actes d'engagement et de réponse, de**

manière à isoler les fonctions et les paramètres les plus sensibles du démonstrateur. Pour calculer engagements et réponses, le témoin dispose du paramètre k et de la clé privée GQ2, c'est-à-dire, de la factorisation du module n selon l'une des trois représentations évoquées ci-dessus. Le

5 Le témoin ainsi isolé est semblable au témoin défini au sein du démonstrateur. Il peut correspondre à une réalisation particulière, par exemple, • une carte à puce reliée à un PC formant ensemble le signataire, ou encore, • des programmes particulièrement protégés au sein d'un PC, ou encore, • des programmes particulièrement protégés au sein d'une carte à puce.

10 1) **L'acte d'engagement** comprend les opérations suivantes.

Lorsque le témoin dispose des m nombres privés Q_1 à Q_m et du module n , il tire au hasard et en privé un ou plusieurs aléas r ($0 < r < n$) ; puis, par k élévations successives au carré (mod n), il transforme chaque aléa r en un engagement R .

$$R \equiv r^v \pmod{n}$$

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m \times f$ composantes privées Q_{ij} , il tire au hasard et en privé une ou plusieurs collections de f aléas : chaque collection comporte un aléa r_i par facteur premier p_i ($0 < r_i < p_i$) ; puis, par k élévations successives au carré (mod p_i),

20 il transforme chaque aléa r_i en une composante d'engagement R_i .

$$R_i \equiv r_i^v \pmod{p_i}$$

Pour chaque collection de f composantes d'engagement, le témoin établit un engagement selon la technique des restes chinois. Il y a autant d'engagements que de collections d'aléas.

$$R = \text{Restes Chinois}(R_1, R_2, \dots, R_f)$$

25 2) **L'acte de défi** consiste à hacher tous les engagements R et le message à signer M pour obtenir un code de hachage à partir duquel le signataire forme un ou plusieurs défis comprenant chacun m défis élémentaires ; chaque défi élémentaire est un nombre de 0 à $v/2-1$; par exemple, avec

$k = 9$ et $m = 8$, chaque défi comporte huit octets. Il y a autant de défis que d'engagements.

$$d = d_1 \ d_2 \ \dots \ d_m, \text{ extraits du résultat Hash}(M, R)$$

3) L'acte de réponse comporte les opérations suivantes.

5 Lorsque la témoin dispose des m nombres privés Q_1 à Q_m et du module n , il calcule une ou plusieurs réponses D en utilisant chaque aléa r de l'acte d'engagement et les nombres privés selon les défis élémentaires.

$$X \equiv Q_1^{d_1} \times Q_2^{d_2} \times \dots \times Q_m^{d_m} \pmod{n}$$

$$D \equiv r \times X \pmod{n}$$

10 Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m \times f$ composantes privées $Q_{i,j}$, il calcule une ou plusieurs collections de f composantes de réponse en utilisant chaque collection d'aléas de l'acte d'engagement : chaque collection de composantes de réponse comporte une composante par facteur premier.

15

$$X_i \equiv Q_{1,i}^{d_1} \times Q_{2,i}^{d_2} \times \dots \times Q_{m,i}^{d_m} \pmod{p_i}$$

$$D_i \equiv r_i \times X_i \pmod{p_i}$$

Pour chaque collection de composantes de réponse, le témoin établit une réponse selon la technique des restes chinois. Il y a autant de réponses que de défis.

20

$$D = \text{Restes Chinois}(D_1, D_2, \dots D_f)$$

Le signataire signe le message M en lui adjoignant un appendice de signature comprenant :

- ou bien, chaque triplet GQ2, c'est-à-dire, chaque engagement R , chaque défi d et chaque réponse D ,
- 25 - ou bien, chaque engagement R et chaque réponse D correspondante,
- ou bien, chaque défi d et chaque réponse D correspondante.

Le déroulement de l'opération de vérification dépend du contenu de l'appendice de signature. On distingue les trois cas.

Au cas où l'appendice comprend un ou plusieurs triplets, l'opération de

contrôle comporte deux processus indépendants dont la chronologie est indifférente. Le contrôleur accepte le message signé si et seulement si les deux conditions suivantes sont remplies.

D'une part, chaque triplet doit être cohérent (une relation appropriée du type suivant doit être vérifiée) et recevable (la comparaison doit se faire sur une valeur non nulle).

$$R \times \prod_{i=1}^m G_i^{d_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k} \times \prod_{i=1}^m G_i^{d_i} \pmod{n}$$

Par exemple, on transforme la réponse D par une séquence d'opérations élémentaires : k carrés (mod n) séparés par $k-1$ multiplications ou divisions (mod n) par des nombres de base. Pour la i ième multiplication ou division, qui s'effectue entre le i ième carré et le $i+1$ ième carré, le i ième bit du défi élémentaire d_1 indique s'il faut utiliser g_1 , le i ième bit du défi élémentaire d_2 indique s'il faut utiliser g_2 , ... jusqu'au i ième bit du défi élémentaire d_m qui indique s'il faut utiliser g_m . On doit ainsi retrouver chaque engagement R présent dans l'appendice de signature.

D'autre part, le ou les triplets doivent être liés au message M . En hachant tous les engagements R et le message M , on obtient un code de hachage à partir duquel on doit retrouver chaque défi d .

$$d = d_1 \ d_2 \ \dots \ d_m, \text{ identiques à ceux extraits du résultat Hash}(M, R)$$

Au cas où l'appendice ne comprend pas de défi, l'opération de contrôle commence par la reconstitution de un ou plusieurs défis d' en hachant tous les engagements R et le message M .

$$d' = d'_1 \ d'_2 \ \dots \ d'_m, \text{ extraits du résultat Hash}(M, R)$$

Ensuite, le contrôleur accepte le message signé si et seulement si chaque triplet est cohérent (une relation appropriée du type suivant est vérifiée) et recevable (la comparaison se fait sur une valeur non nulle).

$$R \times \prod_{i=1}^m G_i^{d'_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k} \times \prod_{i=1}^m G_i^{d'_i} \pmod{n}$$

Au cas où l'appendice ne comprend pas d'engagement, l'opération de contrôle commence par la reconstitution de un ou plusieurs engagements R' selon une des deux formules suivantes, celle qui est appropriée. Aucun engagement rétabli ne doit être nul.

$$5 \quad R' \equiv D^{2^k} / \prod_{i=1}^m G_i^{d_i} \pmod{n} \quad \text{ou bien} \quad R' \equiv D^{2^k} \times \prod_{i=1}^m G_i^{d_i} \pmod{n}$$

Ensuite, le contrôleur doit hacher tous les engagements R' et le message M de façon à reconstituer chaque défis d .

$$d = d_1 \ d_2 \ \dots \ d_m, \quad \text{identiques à ceux extraits du résultat Hash}(M, R')$$

10 Le contrôleur accepte le message signé si et seulement si chaque défi reconstitué est identique au défi correspondant figurant en appendice.

Revendications

1. Procédé destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité et/ou

- l'intégrité d'un message M associé à cette entité,

5 au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- m couples de valeurs privées Q_1, Q_2, \dots, Q_m et publiques G_1, G_2, \dots

G_m (m étant supérieur ou égal à 1),

- un module public n constitué par le produit de f facteurs premiers p_1, p_2, \dots, p_f (f étant supérieur ou égal à 2) ;

10 ledit module et lesdites valeurs privées et publiques étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ ou } G_i \equiv Q_i^v \pmod{n}$$

v désignant un exposant public de la forme :

$$v = 2^k$$

15 où k est un paramètre de sécurité plus grand que 1 ;

lesdites m valeurs publiques G_i étant les carrés g_i^2 de m nombres de base g_1, g_2, \dots, g_m distincts inférieurs aux f facteurs premiers p_1, p_2, \dots, p_f ;

lesdits f facteurs premiers p_1, p_2, \dots, p_f et/ou lesdits m nombres de base g_1, g_2, \dots, g_m étant produits de telle sorte que les conditions suivantes soient

20 satisfaites :

Première condition :

chacune des équations :

$$x^v \equiv g_i^2 \pmod{n} \quad (1)$$

a des solutions en x dans l'anneau des entiers modulo n ;

25 **Deuxième condition :**

dans le cas où $G_i \equiv Q_i^v \pmod{n}$, parmi les m nombres q_i obtenus en élevant Q_i au carré modulo n , $k-1$ fois de rang, l'un d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial),

dans le cas où $G_i \cdot Q_i^v \equiv 1 \pmod{n}$, parmi les m nombres q_i obtenus en

élevant l'inverse de Q_i modulo n au carré modulo n , $k-1$ fois de rang, l'un d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial) ;

Troisième condition :

parmi les $2m$ équations :

$$x^2 \equiv g_i \text{ mod } n \quad (2)$$

$$x^2 \equiv -g_i \text{ mod } n \quad (3)$$

au moins l'une d'entre elles a des solutions en x dans l'anneau des entiers modulo n ;

ledit procédé met en œuvre selon les étapes suivantes une entité appelée témoin disposant des f facteurs premiers p_i et/ou des m nombres de base g_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public n et/ou des m valeurs privées Q_i et/ou des $f.m$ composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \text{ mod } p_j$) des valeurs privées Q_i et de l'exposant public v ;

- le témoin calcule des engagements R dans l'anneau des entiers modulo n ; chaque engagement étant calculé :

- soit en effectuant des opérations du type

$$R \equiv r^v \text{ mod } n$$

où r est un aléa tel que $0 < r < n$,

- soit

•• en effectuant des opérations du type

$$R_i \equiv r_i^v \text{ mod } p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \dots, r_f\}$,

- puis en appliquant la méthode des restes chinois ;

- le témoin reçoit un ou plusieurs défis d ; chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires ; le témoin calcule à partir de chaque défi d une réponse D ,

- soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \text{ mod } n$$

- soit

- en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \bmod p_i$$

- puis en appliquant la méthode des restes chinois ;

5 ledit procédé étant tel qu'il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R**, **d**, **D** constituant un triplet noté **{R, d, D}**.

2. Procédé selon la revendication 1 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur, ladite entité démonstrateur comprenant le témoin ;

10 lesdites entités démonstrateur et contrôleur exécutant les étapes suivantes :

- **étape 1 : acte d'engagement R**

- à chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

15 - le démonstrateur transmet au contrôleur tout ou partie de chaque engagement **R**,

- **étape 2 : acte de défi d**

- le contrôleur, après avoir reçu tout ou partie de chaque engagement **R**, produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur,

- **étape 3 : acte de réponse D**

- le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

- **étape 4 : acte de contrôle**

25 - le démonstrateur transmet chaque réponse **D** au contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R
dans le cas où le démonstrateur a transmis une partie de chaque engagement **R**, le contrôleur, disposant des **m** valeurs publiques **G₁, G₂, ... G_m**, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit

R' satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou a une relation du type,

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n ,$$

5 le contrôleur vérifie que chaque engagement reconstruit R' reproduit tout ou partie de chaque engagement R qui lui a été transmis,
cas où le démonstrateur a transmis l'intégralité de chaque engagement R

10 dans le cas où le démonstrateur a transmis l'intégralité de chaque engagement R , le contrôleur, disposant des m valeurs publiques $G_1, G_2, \dots G_m$, vérifie que chaque engagement R satisfait à une relation du type :

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou a une relation du type,

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n .$$

15 **3. Procédé selon la revendication 1 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message M associé à une entité appelée démonstrateur, ladite entité démonstrateur comprenant le témoin ;**
 lesdites entités démonstrateur et contrôleur exécutant les étapes suivantes :

• **étape 1 : acte d'engagement R**

20 - à chaque appel, le témoin calcule chaque engagement R en appliquant le processus spécifié selon la revendication 1,

• **étape 2 : acte de défi d**

- le démonstrateur applique une fonction de hachage h ayant comme arguments le message M et tout ou partie de chaque engagement R pour
 25 calculer au moins un jeton T ,
 - le démonstrateur transmet le jeton T au contrôleur,
 - le contrôleur, après avoir reçu un jeton T , produit des défis d en nombre égal au nombre d'engagements R et transmet les défis d au démonstrateur,

• **étape 3 : acte de réponse D**

- le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

- le démonstrateur transmet chaque réponse **D** au contrôleur,

5 - le contrôleur, disposant des *m* valeurs publiques **G**₁, **G**₂, ... **G**_{*m*}, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$\mathbf{R}' \equiv \mathbf{G}_1^{d_1} \cdot \mathbf{G}_2^{d_2} \cdot \dots \cdot \mathbf{G}_m^{d_m} \cdot \mathbf{D}^v \bmod n$$

ou à une relation du type :

10
$$\mathbf{R}' \equiv \mathbf{D}^v / \mathbf{G}_1^{d_1} \cdot \mathbf{G}_2^{d_2} \cdot \dots \cdot \mathbf{G}_m^{d_m} \cdot \bmod n$$

- puis le contrôleur applique la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'** pour reconstruire le jeton **T'**,

- puis le contrôleur vérifie que le jeton **T'** est identique au jeton **T** transmis.

15 **4. Procédé selon la revendication 1 destiné à produire la signature numérique d'un message **M** par une entité appelée entité signataire, ladite entité signataire comprenant le témoin ;**

Opération de signature

ladite entité signataire exécute une opération de signature en vue d'obtenir
20 un message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

ladite entité signataire exécute l'opération de signature en mettant en oeuvre
25 les étapes suivantes :

• **étape 1 : acte d'engagement **R****

- à chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

• **étape 2 : acte de défi **d****

- le signataire applique une fonction de hachage **h** ayant comme arguments le message **M** et chaque engagement **R** pour obtenir un train binaire,
- le signataire extrait de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R**,

5 • **étape 3 : acte de réponse D**

- le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1.

5. Procédé selon la revendication 4 destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, le message signé;

10 **Opération de contrôle**

ladite entité contrôleur disposant du message signé exécute une opération de contrôle en procédant comme suit :

- **cas où le contrôleur dispose des engagements R, des défis d, des réponses D,**

15 dans le cas où le contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**,

- • le contrôleur vérifie que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

20
$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

- • le contrôleur vérifie que le message **M**, les défis **d** et les engagements **R** satisfont à la fonction de hachage

25
$$d = h(\text{message}, R)$$

- **cas où le contrôleur dispose des défis d et des réponses D**

dans le cas où le contrôleur dispose des défis **d** et des réponses **D**,

- • le contrôleur reconstruit, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$R' \equiv G_1^{d^1} \cdot G_2^{d^2} \cdot \dots \cdot G_m^{d^m} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d^1} \cdot G_2^{d^2} \cdot \dots \cdot G_m^{d^m} \cdot \text{ mod } n$$

• • le contrôleur vérifie que le message **M** et les défis **d** satisfont à la fonction de hachage

$$d = h(\text{message}, R')$$

• cas où le contrôleur dispose des engagements **R** et des réponses **D**
dans le cas où le contrôleur dispose des engagements **R** et des réponses **D**,

• • le contrôleur applique la fonction de hachage et reconstruit **d'**

$$d' = h(\text{message}, R)$$

• • le contrôleur vérifie que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'^1} \cdot G_2^{d'^2} \cdot \dots \cdot G_m^{d'^m} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'^1} \cdot G_2^{d'^2} \cdot \dots \cdot G_m^{d'^m} \cdot \text{ mod } n$$

6. Système destiné à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou

- l'intégrité d'un message **M** associé à cette entité,

au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées **Q₁, Q₂, ... Q_m** et publiques **G₁, G₂, ...**

G_m (**m** étant supérieur ou égal à 1),

- un module public **n** constitué par le produit de **f** facteurs premiers

p₁, p₂, ... p_f (**f** étant supérieur ou égal à 2),

ledit module et lesdites valeurs privées et publiques étant liés par des

relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \text{ mod } n \text{ ou } G_i \equiv Q_i^v \text{ mod } n$$

v désignant un exposant public de la forme :

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 ;

lesdites m valeurs publiques G_i étant les carrés g_i^2 de m nombres de base g_1, g_2, \dots, g_m distincts inférieurs aux f facteurs premiers p_1, p_2, \dots, p_f ;
 lesdits f facteurs premiers p_1, p_2, \dots, p_f et/ou lesdits m nombres de base g_1, g_2, \dots, g_m étant produits de telle sorte que les conditions suivantes soient satisfaites :

Première condition :

chacune des équations :

$$x^v \equiv g_i^2 \pmod{n} \quad (1)$$

a des solutions en x dans l'anneau des entiers modulo n ;

Deuxième condition :

dans le cas où $G_i \equiv Q_i^v \pmod{n}$, parmi les m nombres q_i obtenus en élevant Q_i au carré modulo n , $k-1$ fois de rang, l'un d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial),

dans le cas où $G_i \cdot Q_i^v \equiv 1 \pmod{n}$, parmi les m nombres q_i obtenus en élevant l'inverse de Q_i modulo n au carré modulo n , $k-1$ fois de rang, l'un d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial) ;

Troisième condition :

parmi les $2m$ équations :

$$x^2 \equiv g_i \pmod{n} \quad (2)$$

$$x^2 \equiv -g_i \pmod{n} \quad (3)$$

au moins l'une d'entre elles a des solutions en x dans l'anneau des entiers modulo n ;

ledit système comprend un dispositif témoin, notamment contenu dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur,

le dispositif témoin comporte

- une zone mémoire contenant les f facteurs premiers p_i et/ou les m nombres de bases g_i et/ou les paramètres des restes chinois des facteurs premiers et/ou le module public n et/ou les m valeurs privées Q_i et/ou les

f.m composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et l'exposant public v ;

ledit dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements R du dispositif témoin, pour calculer des engagements R dans l'anneau des entiers modulo n ; chaque engagement étant calculé :

- soit en effectuant des opérations du type

$$R \equiv r^v \bmod n$$

où r est un aléa produit par les moyens de production d'aléas, r étant tel que $0 < r < n$,

- soit en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \dots, r_t\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois ;

ledit dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis d du dispositif témoin, pour recevoir un ou plusieurs défis d ; chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires ;

- des moyens de calcul, ci après désignés les moyens de calcul des réponses D du dispositif témoin, pour calculer à partir de chaque défi d une réponse D ,

- soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \bmod n$$

- soit en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \bmod p_i$$

puis en appliquant la méthode des restes chinois,

- des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D** ;
il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R**, **d**, **D** constituant un triplet noté **{R, d, D}**.

5 7. Système selon la revendication 6 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur, ledit système étant tel qu'il comporte

- un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des
10 moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

- un dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un
15 serveur distant, ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement; électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;
ledit système permettant d'exécuter les étapes suivantes :

20 • **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre
25 tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour

transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion ;

• **étape 2 : acte de défi d**

le dispositif contrôleur comporte des moyens de production de défis pour
5 produire, après avoir reçu tout ou partie de chaque engagement **R**, des défis **d** en nombre égal au nombre d'engagements **R**,

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion ;

10 • **étape 3 : acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin, calculent les
15 réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur,

20 le dispositif contrôleur comporte aussi

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

25 **cas où le démonstrateur a transmis une partie de chaque engagement R**
dans le cas où les moyens de transmission du démonstrateur ont transmis une partie de chaque engagement **R**, les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques **G**₁, **G**₂, ... **G**_m, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit

R' satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n ,$$

5 les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit R' à tout ou partie de chaque engagement R reçu, **cas où le démonstrateur a transmis l'intégralité de chaque engagement R**

10 dans le cas où les moyens de transmission du démonstrateur ont transmis l'intégralité de chaque engagement R , les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des m valeurs publiques G_1, G_2, \dots, G_m , vérifient que chaque engagement R satisfait à une relation du type :

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

15 ou à une relation du type,

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n .$$

8. Système selon la revendication 6 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message M associé à une entité appelée démonstrateur,

20 ledit système étant tel qu'il comporte

- un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

25 - un dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant, ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement; électromagnétiquement,

optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;

ledit système permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

5 à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre
10 tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion,

• **étape 2 : acte de défi d**

le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du démonstrateur, appliquant une fonction de
15 hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer au moins un jeton **T**,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif démonstrateur, pour transmettre chaque jeton **T**, via les moyens de connexion, au dispositif
20 contrôleur,

le dispositif contrôleur comporte aussi des moyens de production de défis pour produire, après avoir reçu le jeton **T**, des défis **d** en nombre égal au nombre d'engagements **R**,

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les
25 défis **d** au démonstrateur, via les moyens de connexion ;

• **étape 3 : acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens

d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

5 • **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur,

le dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques **G**₁, **G**₂, ... **G**_m, pour d'une part, calculer à partir de
10 chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à une relation du type :

15
$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

puis d'autre part, calculer en appliquant la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'**, un jeton **T'**,

le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour
20 comparer le jeton calculé **T'** au jeton **T** reçu.

9. Système selon la revendication 6 destiné à produire la signature numérique d'un message **M**, ci-après désigné le message signé, par une entité appelée entité signataire ;

25 le message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

Opération de signature

ledit système étant tel qu'il comporte un dispositif signataire associé à l'entité signataire, ledit dispositif signataire étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit système permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion,

• **étape 2 : acte de défi d**

le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R**,

• **étape 3 : acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion,

les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre

les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

10. Système selon la revendication 9 destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, le message signé;

Opération de contrôle

ledit système étant tel qu'il comporte un dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant, ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif signataire ; le dispositif signataire associé à l'entité signataire comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif signataire, pour transmettre au dispositif contrôleur, le message signé, via les moyens de connexion, de telle sorte que le dispositif contrôleur dispose d'un message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,
- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

• **cas où le dispositif contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**,**

dans le cas où le dispositif contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**,

- les moyens de calcul et de comparaison du dispositif contrôleur

vérifient que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à des relations du type :

5
$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M**, les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$d = h(\text{message}, R)$$

10 • cas où le dispositif contrôleur dispose des défis **d** et des réponses **D**

dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D**,

• • les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

15
$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M** et les défis **d** satisfont à la fonction de hachage

20
$$d = h(\text{message}, R')$$

• cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D**

dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D**,

25 • • les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$d' = h(\text{message}, R)$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à

des relations du type :

$$R \equiv G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot \bmod n$$

5 **11.** Dispositif terminal associé à une entité, se présentant notamment sous la forme d'un objet nomade par exemple sous la forme d'une carte bancaire à microprocesseur, destiné à prouver à un dispositif contrôleur,

- l'authenticité de l'entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

10 au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées Q_1, Q_2, \dots, Q_m et publiques G_1, G_2, \dots, G_m (**m** étant supérieur ou égal à 1),

- un module public **n** constitué par le produit de **f** facteurs premiers p_1, p_2, \dots, p_f (**f** étant supérieur ou égal à 2),

15 ledit module et lesdites valeurs privées et publiques étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n$$

v désignant un exposant public de la forme :

$$v = 2^k$$

20 où **k** est un paramètre de sécurité plus grand que 1 ;

lesdites **m** valeurs publiques G_i étant les carrés g_i^2 de **m** nombres de base g_1, g_2, \dots, g_m distincts inférieures aux **f** facteurs premiers p_1, p_2, \dots, p_f ;

lesdits **f** facteurs premiers p_1, p_2, \dots, p_f et/ou lesdits **m** nombres de base g_1, g_2, \dots, g_m étant produits de telle sorte que les conditions suivantes soient

25 satisfaites :

Première condition :

chacune des équations :

$$x^v \equiv g_i^2 \bmod n \quad (1)$$

a des solutions en **x** dans l'anneau des entiers modulo **n** ;

Deuxième condition :

dans le cas où $G_i \equiv Q_i^v \text{ mod } n$, parmi les m nombres q_i obtenus en élevant Q_i au carré modulo n , $k-1$ fois de rang, l'un d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial),

5 dans le cas où $G_i \cdot Q_i^v \equiv 1 \text{ mod } n$, parmi les m nombres q_i obtenus en élevant l'inverse de Q_i modulo n au carré modulo n , $k-1$ fois de rang, l'un d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial) ;

Troisième condition :

parmi les $2m$ équations :

10
$$x^2 \equiv g_i \text{ mod } n \quad (2)$$

$$x^2 \equiv -g_i \text{ mod } n \quad (3)$$

au moins l'une d'entre elles a des solutions en x dans l'anneau des entiers modulo n ;

ledit dispositif terminal comprend un dispositif témoin comportant - -

15 - une zone mémoire contenant les f facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou le module public n et/ou les m nombres de base g_i et/ou les m valeurs privées Q_i et/ou les $f.m$ composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \text{ mod } p_j$) des valeurs privées Q_i et l'exposant public v ;

20 ledit dispositif témoin comporte aussi

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements R du dispositif témoin, pour calculer des engagements R dans l'anneau des entiers modulo n ; chaque engagement étant calculé :

25

- soit en effectuant des opérations du type

$$R \equiv r^v \text{ mod } n$$

ou r est un aléa produit par les moyens de production d'aléas, r étant tel que $0 < r < n$,

- soit en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

ou r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \dots, r_t\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois ;

ledit dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis d du dispositif témoin, pour recevoir un ou plusieurs défis d ; chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires ;

- des moyens de calcul, ci après désignés les moyens de calcul des réponses D du dispositif témoin, pour calculer à partir de chaque défi d une réponse D ,

- soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot \dots \cdot Q_m^{d_m} \bmod n$$

- soit en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \bmod p_i$$

puis en appliquant la méthode des restes chinois,

- des moyens de transmission pour transmettre un ou plusieurs engagements R et une ou plusieurs réponses D ;

il y a autant de réponses D que de défis d que d'engagements R , chaque groupe de nombres R, d, D constituant un triplet noté $\{R, d, D\}$.

12. Dispositif terminal selon la revendication 11 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur,

ledit dispositif terminal étant tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur

dans une carte bancaire à microprocesseur,
ledit dispositif démonstrateur comportant des moyens de connexion pour le
connecter électriquement, électromagnétiquement, optiquement ou de
manière acoustique, notamment via un réseau de communication
informatique, au dispositif contrôleur associé à l'entité contrôleur, ledit
5 dispositif contrôleur se présentant notamment sous la forme d'un terminal
ou d'un serveur distant ;

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

10 à chaque appel, les moyens de calcul des engagements **R** du dispositif
témoin calculent chaque engagement **R** en appliquant le processus spécifié
selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après
désignés les moyens de transmission du dispositif témoin, pour transmettre
15 tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les
moyens d'interconnexion,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-
après désignés les moyens de transmission du démonstrateur, pour
transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur,
20 via les moyens de connexion ;

• **étapes 2 et 3 : acte de défi d, acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque
défi **d** provenant du dispositif contrôleur via les moyens de connexion entre
le dispositif contrôleur et le dispositif démonstrateur et via les moyens
25 d'interconnexion entre le dispositif démonstrateur et le dispositif témoin,

les moyens de calcul des réponses **D** du dispositif témoin, calculent les
réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la
revendication 1,

• **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle,

13. Dispositif terminal selon la revendication 11 destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur,

ledit dispositif terminal étant tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit dispositif démonstrateur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion,

• **étapes 2 et 3 : acte de défi d, acte de réponse D**

le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du démonstrateur, appliquant une fonction de

hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer au moins un jeton **T**,

le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif démonstrateur, pour transmettre chaque jeton **T**, via les moyens de connexion, au dispositif contrôleur,

*(ledit dispositif contrôleur produit, après avoir reçu le jeton **T**, des défis **d** en nombre égal au nombre d'engagements **R**,)*

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin, les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la revendication 1,

• **étape 4 : acte de contrôle**

les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

14. Dispositif terminal selon la revendication 11 destiné à produire la signature numérique d'un message **M**, ci-après désigné le message signé, par une entité appelée entité signataire ;
le message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** ;

ledit dispositif terminal étant tel qu'il comporte un dispositif signataire associé à l'entité signataire, ledit dispositif signataire étant interconnecté au dispositif témoin par des moyens d'interconnexion et pouvant se présenter notamment sous la forme de microcircuits logiques dans un objet nomade

par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur,

ledit dispositif signataire comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur, ledit dispositif contrôleur se présentant notamment sous la forme d'un terminal ou d'un serveur distant ;

Opération de signature

ledit dispositif terminal permettant d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

à chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié selon la revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion,

- **étape 2 : acte de défi d**

le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R**, pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R**,

- **étape 3 : acte de réponse D**

les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion, les moyens de calcul des réponses **D** du dispositif témoin, calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié selon la

revendication 1,

le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

5 **15.** Dispositif contrôleur, se présentant notamment sous la forme d'un terminal ou d'un serveur distant, associé à une entité contrôleur, destiné à contrôler :

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

10 au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs publiques $G_1, G_2, \dots G_m$ (**m** étant supérieur ou égal à 1),

- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \dots p_f$ (**f** étant supérieur ou égal à 2) inconnus du dispositif contrôleur et de l'entité contrôleur associé,

15 ledit module et lesdites valeurs privées et publiques étant liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ ou } G_i \equiv Q_i^v \pmod{n}$$

v désignant un exposant public de la forme :

$$v = 2^k$$

20 où **k** est un paramètre de sécurité plus grand que 1 ;

où Q_i désigne une valeur privée, inconnue du dispositif contrôleur, associée à la valeur publique G_i ;

lesdites **m** valeurs publiques G_i étant les carrés g_i^2 de **m** nombres de base

25 $g_1, g_2, \dots g_m$ distincts inférieures aux **f** facteurs premiers $p_1, p_2, \dots p_f$;

lesdits **f** facteurs premiers $p_1, p_2, \dots p_f$ et/ou lesdits **m** nombres de base $g_1, g_2, \dots g_m$ étant produits de telle sorte que les conditions suivantes soient satisfaites :

Première condition :

chacune des équations :

$$x^y \equiv g_i^2 \text{ mod } n \quad (1)$$

a des solutions en x dans l'anneau des entiers modulo n ;

Deuxième condition :

5 dans le cas où $G_i \equiv Q_i^y \text{ mod } n$, parmi les m nombres q_i obtenus en élevant Q_i au carré modulo n, k-1 fois de rang, l'un d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial),

dans le cas où $G_i \cdot Q_i^y \equiv 1 \text{ mod } n$, parmi les m nombres q_i obtenus en élevant l'inverse de Q_i modulo n au carré modulo n, k-1 fois de rang, l'un
10 d'entre eux est différent de $\pm g_i$ (c'est-à-dire est non trivial) ;

Troisième condition :

parmi les 2m équations :

$$x^2 \equiv g_i \text{ mod } n \quad (2)$$

$$x^2 \equiv -g_i \text{ mod } n \quad (3)$$

15 au moins l'une d'entre elles a des solutions en x dans l'anneau des entiers modulo n .

16. Dispositif contrôleur selon la revendication 15 destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur ;

20 ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associée à l'entité démonstrateur ;

25 ledit dispositif contrôleur permettant d'exécuter les étapes suivantes :

• **étapes 1 et 2 : acte d'engagement R, acte de défi d**

ledit dispositif contrôleur comporte aussi des moyens de réception de tout ou partie des engagements **R** provenant du dispositif démonstrateur, via les moyens de connexion,

le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu tout ou partie de chaque engagement R , des défis d en nombre égal au nombre d'engagements R , chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires,

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis d au démonstrateur, via les moyens de connexion ;

• **étapes 3 et 4 : acte de réponse D , acte de contrôle**

ledit dispositif contrôleur comporte aussi :

- des moyens de réception des réponses D provenant du dispositif démonstrateur, via les moyens de connexion

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

cas où le démonstrateur a transmis une partie de chaque engagement R
 dans le cas où les moyens de réception du dispositif contrôleur ont reçus une partie de chaque engagement R , les moyens de calcul du dispositif contrôleur, disposant des m valeurs publiques G_1, G_2, \dots, G_m , calculent à partir de chaque défi d et de chaque réponse D un engagement reconstruit R' satisfaisant à une relation du type :

$$R' \equiv G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot \bmod n ,$$

les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit R' à tout ou partie de chaque engagement R reçu,

cas où le démonstrateur a transmis l'intégralité de chaque engagement R

dans le cas où les moyens de réception du dispositif contrôleur ont reçus

l'intégralité de chaque engagement R , les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des m valeurs publiques G_1, G_2, \dots, G_m , vérifient que chaque engagement R satisfait à une relation du type :

$$R \equiv G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot D^v \text{ mod } n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot \text{mod } n.$$

17. Dispositif contrôleur selon la revendication 15 destiné à prouver l'intégrité d'un message M associé à une entité appelée démonstrateur, ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associée à l'entité démonstrateur ;

ledit dispositif contrôleur permettant d'exécuter les étapes suivantes :

• **étapes 1 et 2 : acte d'engagement R , acte de défi d**

ledit dispositif contrôleur comporte aussi des moyens de réception de jetons T provenant du dispositif démonstrateur, via les moyens de connexion, le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu le jeton T , des défis d en nombre égal au nombre d'engagements R , chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires ;

le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis d au démonstrateur, via les moyens de connexion ;

• **étapes 3 et 4 : acte de réponse D , acte de contrôle**

ledit dispositif contrôleur comporte aussi :

- des moyens de réception des réponses D provenant du dispositif démonstrateur, via les moyens de connexion,

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des m valeurs publiques $G_1, G_2, \dots G_m$, pour d'une part, calculer à partir de chaque défi d et de chaque réponse D un engagement reconstruit R' satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots G_m^{dm} \cdot D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots G_m^{dm} \cdot \bmod n$$

puis d'autre part, calculer en appliquant une fonction de hachage h ayant comme arguments le message M et tout ou partie de chaque engagement reconstruit R' , un jeton T' ,

le dispositif contrôleur comporte aussi

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton calculé T' au jeton T reçu.

18. Dispositif contrôleur selon la revendication 15 destiné à prouver l'authenticité du message M en contrôlant, par une entité appelée contrôleur, un message signé;

le message signé, émis par un dispositif signataire associé à une entité signataire disposant d'une fonction de hachage h (message, R), comprenant :

- le message M ,
- des défis d et/ou des engagements R ,
- des réponses D ;

Opération de contrôle

ledit dispositif contrôleur comportant des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif signataire associée à l'entité signataire ;
ledit dispositif contrôleur ayant reçu le message signé du dispositif

signataire, via les moyens de connexion,

le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur,

• **cas où le dispositif contrôleur dispose des engagements R , des défis d , des réponses D ,**

dans le cas où le dispositif contrôleur dispose des engagements R , des défis d , des réponses D ,

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements R , les défis d et les réponses D satisfont à des relations du type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

• • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message M , les défis d et les engagements R satisfont à la fonction de hachage

$$d = h(\text{message}, R)$$

• **cas où le dispositif contrôleur dispose des défis d et des réponses D**

dans le cas où le dispositif contrôleur dispose des défis d et des réponses D ,

• • les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi d et de chaque réponse D , des engagements R' satisfaisant à des relations du type :

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

ou à des relations du type :

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

• • les moyens de calcul et de comparaison du dispositif contrôleur

vérifient que le message **M** et les défis **d** satisfont à la fonction de hachage

$$d = h(\text{message}, R')$$

• cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D**

5 dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D**,

• les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$d' = h(\text{message}, R)$$

10 • les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot D^v \bmod n$$

ou à des relations du type :

15
$$R \equiv D^v / G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot \bmod n$$

1/3

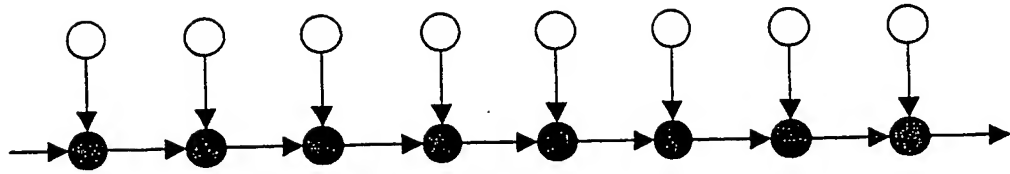


Fig.1A

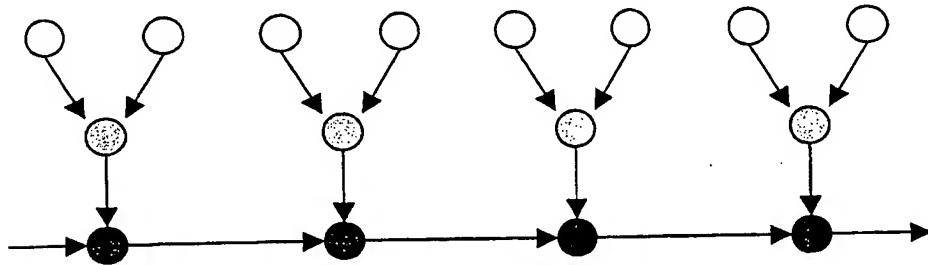


Fig.1B

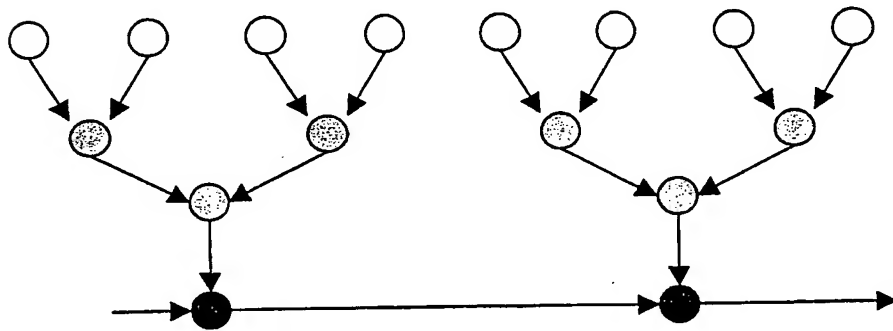


Fig.1C

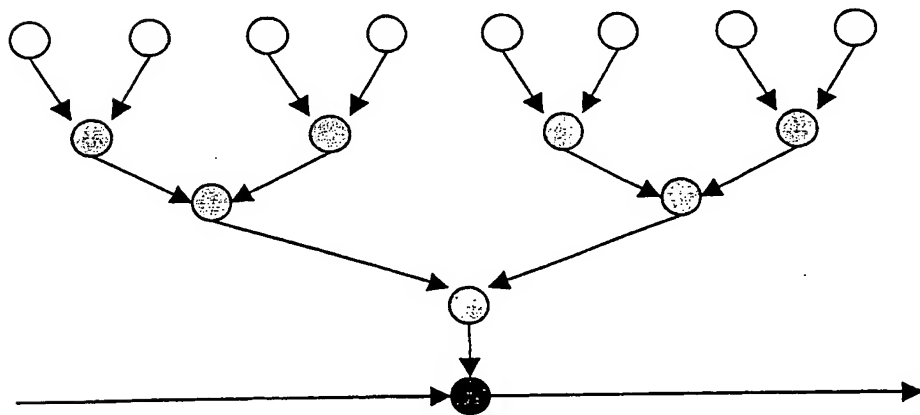


Fig.1D

THIS PAGE BLANK (USPTO)

2/3

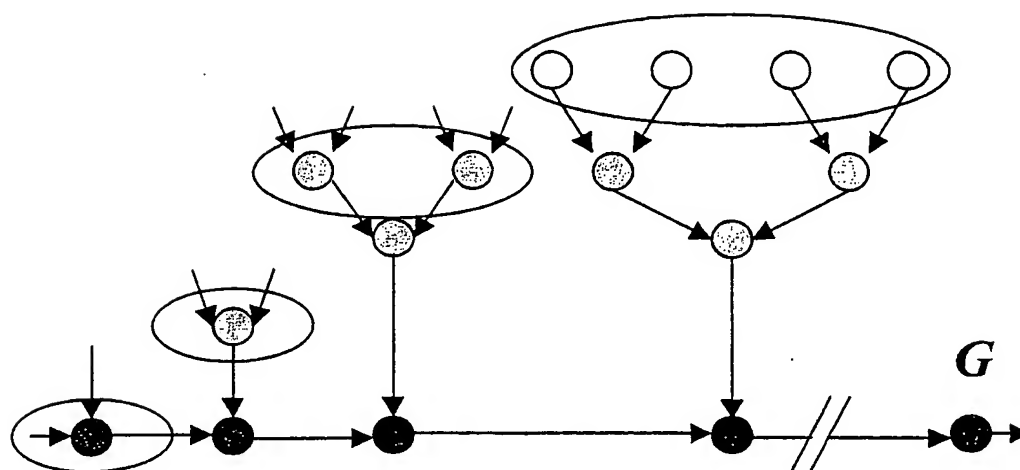


Fig.2A

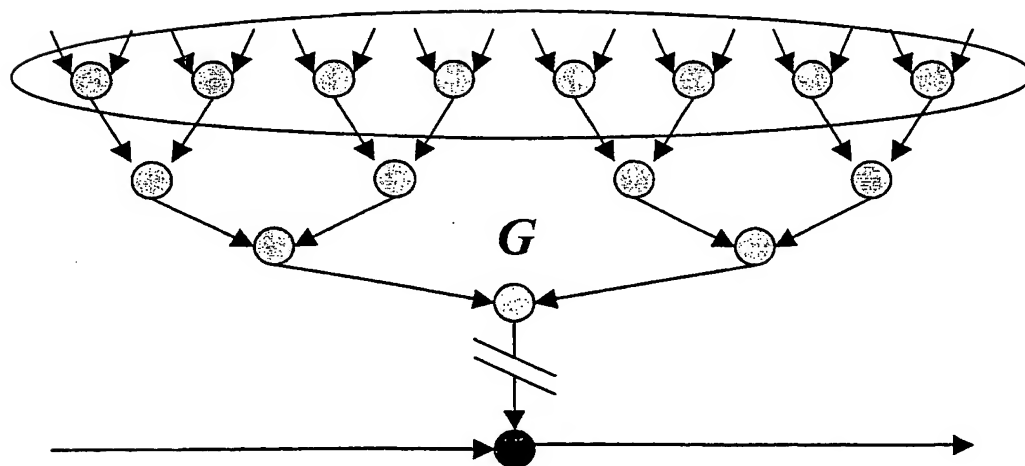
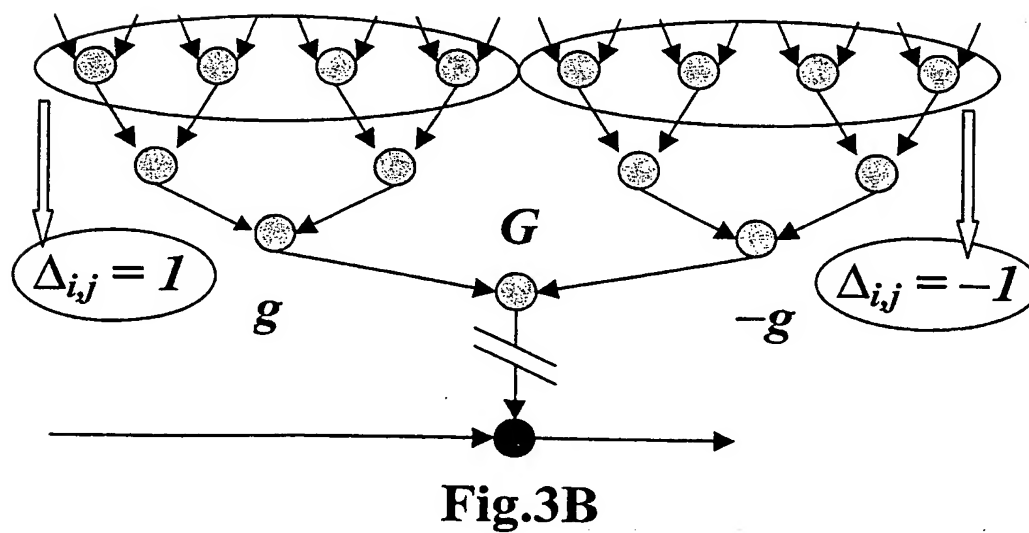
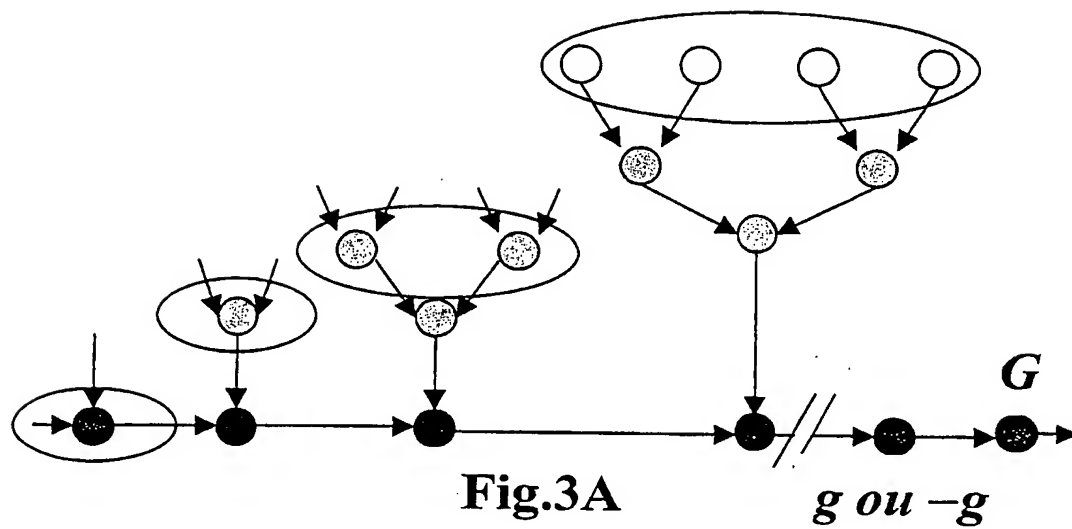


Fig.2B

THIS PAGE BLANK (USPTO)

3/3



THIS PAGE BLANK (USPTO)